

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 9 月 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 1 4 4 6 5
Application Number:

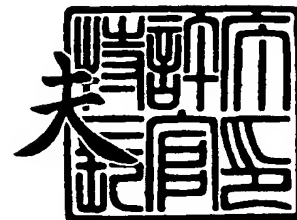
[ST. 10/C] : [J P 2 0 0 3 - 3 1 4 4 6 5]

出 願 人 株式会社リコー
Applicant(s):

2 0 0 3 年 1 0 月 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 0304621
【提出日】 平成15年 9月 5日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G06F 17/60
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 斉藤 敦久
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 金井 洋一
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 谷内田 益義
【特許出願人】
 【識別番号】 000006747
 【氏名又は名称】 株式会社リコー
【代理人】
 【識別番号】 100070150
 【弁理士】
 【氏名又は名称】 伊東 忠彦
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-273985
 【出願日】 平成14年 9月19日
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-275973
 【出願日】 平成14年 9月20日
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-297888
 【出願日】 平成14年10月10日
【手数料の表示】
 【予納台帳番号】 002989
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9911477

【書類名】 特許請求の範囲**【請求項 1】**

ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手段と、

外部からのセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手段と、

上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有することを特徴とする画像形成装置。

【請求項 2】

ネットワークを介して通信制御を行う通信手段を有し、

上記ポリシー書き換え手段は、上記通信手段によって受信したセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えることを特徴とする請求項 1 記載の画像形成装置。

【請求項 3】

上記ポリシー書き換え手段は、電源投入時に上記通信手段によって、外部から取得したセキュリティポリシーを上記ポリシー保持手段に書き込むことを特徴とする請求項 2 記載の画像形成装置。

【請求項 4】

上記ポリシー保持手段にて保持される上記セキュリティポリシーの書き換えタイミングを上記通信手段に通知するタイマー手段を有し、

上記通信手段は、上記ネットワークを介して、上記セキュリティポリシーを配布するポリシー配布サーバから該セキュリティポリシーを取得することを特徴とする請求項 2 又は 3 記載の画像形成装置。

【請求項 5】

セキュリティポリシーを記憶した記憶媒体から該セキュリティポリシーを読み出すインターフェース手段を有し、

上記インターフェース手段によって読み出されたセキュリティポリシーによって、上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えることを特徴とする請求項 1 記載の画像形成装置。

【請求項 6】

ネットワークを介して通信制御を行う通信手段を有し、

上記通信手段は、セキュリティポリシーの選択を示す選択情報を受信すると、上記ポリシー書き換え手段に通知し、

上記ポリシー書き換え手段は、上記選択情報に基づいて、上記インターフェース手段によって読み出されたセキュリティポリシーによって、上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えることを特徴とする請求項 5 記載の画像形成装置。

【請求項 7】

上記ポリシー保持手段は、複数のセキュリティポリシーを保持し、

上記ポリシー書き換え手段は、上記選択情報に基づいて、上記ポリシー保持手段で保持される上記複数のセキュリティポリシーの 1 つを施行すべきセキュリティポリシーとして設定することを特徴とする請求項 6 記載の画像形成装置。

【請求項 8】

上記通信手段は、上記ネットワークを介して、Simple Object Access Protocolに従って上記セキュリティポリシーを取得することを特徴とする請求項 2 又は 6 記載の画像形成装置。

【請求項 9】

ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手段と、

外部からのセキュリティポリシーで上記ポリシー保持手順にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手順と、

上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手順とをコンピュータが実行することを特徴とする方法。

【請求項 1 0】

ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手順と、

外部からのセキュリティポリシーで上記ポリシー保持手順にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手順と、

上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手順とをコンピュータに実行させることを特徴とするコンピュータ実行可能なプログラム。

【請求項 1 1】

ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手順と、

外部からのセキュリティポリシーで上記ポリシー保持手順にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手順と、

上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手順とをコンピュータに実行させることを特徴とするプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 1 2】

ネットワークを介して通信制御を行う通信手段と、

ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを管理するポリシー管理手段とを有し、

上記通信手段は、上記ポリシー管理手段によって管理される上記セキュリティポリシーを上記ネットワークを介して接続される装置へ配布することを特徴とするポリシー配布サーバ。

【請求項 1 3】

上記通信手段は、上記セキュリティポリシーを配布する際に、認証情報を同時に送信することを特徴とする請求項 1 2 記載のポリシー配布サーバ。

【請求項 1 4】

上記通信手段は、上記ネットワークを介して接続される上記装置から上記ポリシー管理手段によって管理される上記セキュリティポリシーの取得要求と共に、該装置の認証情報を受信し、該認証情報に基づいた認証結果に従って、該装置へ該セキュリティポリシーを送信することを特徴とするポリシー配布サーバ。

【請求項 1 5】

記憶媒体へ上記セキュリティポリシーを書き込むインターフェースを有し、

上記ポリシー管理手段は、上記インターフェースによって、上記セキュリティポリシーを上記記憶媒体に書き込むことを特徴とする請求項 1 2 乃至 1 4 のいずれか一項記載のポリシー配布サーバ。

【請求項 1 6】

ドキュメントに関するドキュメント属性を、該ドキュメント属性に基づいて該ドキュメントに関する取り扱いのルールを提供する外部サーバへ送信することによって、該外部サーバから上記ルールを取得するルール取得手段と、

上記ルール取得手段によって取得された上記ルールに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有することを特徴とする画像形成装置。

【請求項 1 7】

上記ルール取得手段は、上記外部サーバとの通信を Simple Object Access Protocol に従って制御する通信手段を有することを特徴とする請求項 1 6 記載の画像形成装置。

【請求項 1 8】

上記ルール取得手段は、
上記外部サーバとの通信を制御する通信手段と、
選択可能な機能の実行可否を示す実行可否情報を保持する選択機能保持手段と、
上記選択機能保持手段によって保持される上記実行可否情報を参照することによって、
上記ルールによって指定される上記動作を許可するために満たすべき動作要件を実行できるか否かを判断する動作要件判断手段とを有し、
上記動作制御手段は、上記動作要件判断手段による判断結果に基づいて、上記ドキュメントに対する動作を制御することを特徴とする請求項 1 6 記載の画像形成装置。

【請求項 1 9】

ネットワークを介して通信制御を行う通信手段と、
ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持する保持手段と、
ドキュメント属性と上記ドキュメントに対して実行される動作とに基づいて、上記保持手段によって保持される上記セキュリティポリシーを参照し、該ドキュメントへの該動作に対する上記ルールを取得するポリシー取得手段とを有し、
上記通信手段は、上記ネットワークを介して受信した上記ドキュメント属性と上記動作とを上記ポリシー取得手段に通知し、上記ポリシー取得手段が取得した上記ルールを送信することを特徴とするポリシー解釈サーバ。

【請求項 2 0】

上記ネットワークを介して接続される装置毎に選択可能な機能の実行可否を示す実行可否情報を保持する選択機能保持手段と、
上記選択機能保持手段によって保持される上記実行可否情報を参照することによって、上記ポリシー取得手段によって取得した上記ルールによって指定される上記動作を許可するために満たすべき動作要件を実行可能か否かを判断する動作要件判断手段とを有することを特徴とする請求項 1 9 記載のポリシー解釈サーバ。

【書類名】 明細書**【発明の名称】 画像形成装置及びポリシー配布サーバ並びにポリシー解釈サーバ****【技術分野】****【0001】**

本発明は、情報システムのセキュリティを確保するシステムに関し、特に、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う画像形成装置に関する。

【0002】

また、本発明は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う装置にセキュリティポリシーを配布するポリシー配布サーバに関する。

【0003】

更に、本発明は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいて、ネットワークを介して接続される装置に、該ドキュメントに対する動作を許可するための動作要件を提供するポリシー解釈サーバに関する。

【背景技術】**【0004】**

オフィスに代表されるようなドキュメントを扱うフィールドでは、そのドキュメントのセキュリティをコントロールしたいという要望が、常に存在する。例えば秘密の文書を複写する際には管理責任者の許可を得なければならない等、特に情報のコンテナであるドキュメントに対するポリシー、中でも機密保持に関するポリシーの制御が重要視される。一般に、情報システムのセキュリティ確保は機密性、完全性、可用性の確保に大別されるが、完全性や可用性はシステムの管理者が適切に運営、管理すれば実質上問題のないレベルまで確保できることが多い。これに対して、機密性の確保のためには、ユーザ組織に所属するメンバに、ポリシーを共有及び徹底させなければならないためであろうと推測される。

【0005】

現実に多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。

【0006】

セキュリティポリシーに基づいてアクセス制御を行う方法に関する従来技術としては、種々のものが挙げられる（特許文献1から、特許文献14）。

【0007】

例えば、アクセス制御において、条件付のアクセス許可を評価することが記載されている（特許文献1）。

【0008】

また、例えば、情報セキュリティポリシーに従った企業情報システムのセキュリティ管理、監査の簡単化について記載されている（特許文献2）。

【0009】

しかし、特に、上述の特許文献1では、データファイルへのアクセス制御システムで、アクセス後のデータの処理、特に読み取りなどには言及されていない。

【0010】

また、上述の特許文献2では、セキュリティポリシー、システム、制御手段から構成され、それぞれの組み合わせを登録してあるDB（データベース）から制御手段を抽出して、システムをポリシーに合うように制御する手段を有しているがしかし、その状態を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低い。

【0011】

また、特許文献7の操作者IDを入力させ、文書からIDを取り出し、複写を制御する方法では、複写を拒否する、又は、複写を許可してログを記録するという固定されたルールに基づく制御しか行えない。

【0012】

特許文献8の画像から機密文書であることを示すマークを取り出してチェックする方法では、得られた情報からどのような動作を行うか否かが決められているため、ルールの柔軟性に欠ける。

【0013】

特許文献9の印刷情報に含まれる出力制限データに基づいて出力先を制御する方法では、印刷情報にルールを含めなければならない。

【0014】

特許文献10の画像を読み取ってパスワードとともに記憶し、出力の際にパスワードが一致したときに許可する方法では、判断する基準がパスワードだけであり、それによって制御される動作も許可、又は、不許可だけである。

【0015】

特許文献11のネットワーク上の複数のMFPのうち、一つのMFPがユーザ管理を行ってネットワーク上のMFPすべての操作の許可、不許可を制御する方法では、制御される動作は許可、又は、不許可だけである。

【0016】

特許文献12の複数の機器について利用の許可、操作の許可をユーザごとに判断する方法では、許可、不許可だけしか制御できないし、ユーザ情報に基づいた制御しかできない。というように、従来技術の問題点はルールが限定的で柔軟性がなく、またそのルールもあらかじめ決められたものだけであるという欠点がある。すなわち、従来の入出力装置は、「ユーザ」と「ドキュメント」のIDに対する、操作の「許可」、「禁止」だけを、「あらかじめ」決められているものばかりである。

【特許文献1】特開2001-184264号公報

【特許文献2】特開2001-273388号公報

【特許文献3】特開2001-337864号公報

【特許文献4】特開平09-293036号公報

【特許文献5】特開平07-141296号公報

【特許文献6】特許第02735966号公報

【特許文献7】特許3203103号公報

【特許文献8】特開平7-58950号公報

【特許文献9】特開平7-152520号公報

【特許文献10】特開平10-191072号公報

【特許文献11】特開2000-15898号公報

【特許文献12】特開2000-357064号公報

【特許文献13】特開2001-125759号公報

【特許文献14】特開2001-325249号公報。

【発明の開示】

【発明が解決しようとする課題】

【0017】

このようなセキュリティの実施方法では、ドキュメントの印刷に対するセキュリティを実行する場合には、第1に、セキュリティの施行者が、さまざまな機器のセキュリティに関する知識を必要とする。そして、第2には、すべての機器に対してセキュリティが、一つ一つ実行される必要がある。第3には、システムの全体がどのようなセキュリティ状態になっているのかを容易に把握することが必要であるが、把握しにくい。そして、第4に、個々の機器にセキュリティが実施されていても、実際に文書のセキュリティが守られていることが実感できない。このように、実際のオフィスシステムにおけるセキュリティの確保については、以上のような問題点がある。

【0018】

本発明は、上述の問題点を解決することを目的とする。

【0019】

特に本発明の第一の目的は、ネットワークを介して外部サーバから配布されるドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいて処理制御を行う画像形成装置を提供することである。

【0020】

また、本発明の第二の目的は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う装置にセキュリティポリシーを配布するポリシー配布サーバを提供することである。

【0021】

更に、本発明の第三の目的は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいて、ネットワークを介して接続される装置に、該ドキュメントに対する動作を許可するための動作要件を提供するポリシー解釈サーバを提供することである。

【課題を解決するための手段】**【0022】**

上記第一の課題を解決するため、本発明は、請求項1に記載されるように、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手段と、外部からのセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手段と、上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有するように構成される。

【0023】

このような画像形成装置では、外部から提供されるセキュリティポリシーで既存のセキュリティポリシーを書き換えることができる。

【0024】

また、本発明は、請求項2に記載されるように、ネットワークを介して通信制御を行う通信手段を有し、上記ポリシー書き換え手段は、上記通信手段によって受信したセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるように構成することができる。

【0025】

また、本発明は、請求項3に記載されるように、上記ポリシー書き換え手段は、電源投入時に上記通信手段によって、外部から取得したセキュリティポリシーを上記ポリシー保持手段に書き込むように構成することができる。

【0026】

また、本発明は、請求項4に記載されるように、上記ポリシー保持手段にて保持される上記セキュリティポリシーの書き換えタイミングを上記通信手段に通知するタイマー手段を有し、上記通信手段は、上記ネットワークを介して、上記セキュリティポリシーを配布するポリシー配布サーバから該セキュリティポリシーを取得するように構成することができる。

【0027】

また、本発明は、請求項5に記載されるように、セキュリティポリシーを記憶した記憶媒体から該セキュリティポリシーを読み出すインターフェース手段を有し、上記インターフェース手段によって読み出されたセキュリティポリシーによって、上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるように構成することができる。

【0028】

また、本発明は、請求項6に記載されるように、ネットワークを介して通信制御を行う通信手段を有し、上記通信手段は、セキュリティポリシーの選択を示す選択情報を受信すると、上記ポリシー書き換え手段に通知し、上記ポリシー書き換え手段は、上記選択情報

に基づいて、上記インターフェース手段によって読み出されたセキュリティポリシーによって、上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるように構成することができる。

【0029】

また、本発明は、請求項7に記載されるように、上記ポリシー保持手段は、複数のセキュリティポリシーを保持し、上記ポリシー書き換え手段は、上記選択情報に基づいて、上記ポリシー保持手段で保持される上記複数のセキュリティポリシーの1つを施行すべきセキュリティポリシーとして設定するように構成することができる。

【0030】

また、本発明は、請求項8に記載されるように、上記通信手段は、上記ネットワークを介して、Simple Object Access Protocolに従って上記セキュリティポリシーを取得するように構成することができる。

【0031】

上記第一の課題を解決するための手段として、本発明は、上記画像形成装置での処理を行う方法、その処理コンピュータに実行させるためのプログラム、及び、そのプログラムを記憶した記憶媒体とすることもできる。

【0032】

また、上記第二の課題を解決するために、本発明は、請求項12に記載されるように、ネットワークを介して通信制御を行う通信手段と、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを管理するポリシー管理手段とを有し、上記通信手段は、上記ポリシー管理手段によって管理される上記セキュリティポリシーを上記ネットワークを介して接続される装置へ配布するように構成される。

【0033】

このようなポリシー配布サーバは、ネットワークを介して接続される複数の装置に対して、同一のセキュリティポリシーを配布することができる。

【0034】

また、本発明は、請求項13に記載されるように、上記通信手段は、上記セキュリティポリシーを配布する際に、認証情報を同時に送信するように構成することができる。

【0035】

また、本発明は、請求項14に記載されるように、上記通信手段は、上記ネットワークを介して接続される上記装置から上記ポリシー管理手段によって管理される上記セキュリティポリシーの取得要求と共に、該装置の認証情報とを受信し、該認証情報に基づいた認証結果に従って、該装置へ該セキュリティポリシーを送信するように構成することができる。

【0036】

また、本発明は、請求項15に記載されるように、記憶媒体へ上記セキュリティポリシーを書き込むインターフェースを有し、上記ポリシー管理手段は、上記インターフェースによって、上記セキュリティポリシーを上記記憶媒体に書き込むように構成することができる。

【0037】

また、本発明は、請求項16に記載されるように、ドキュメントに関するドキュメント属性を、該ドキュメント属性に基づいて該ドキュメントに関する取り扱いのルールを提供する外部サーバへ送信することによって、該外部サーバから上記ルールを取得するルール取得手段と、上記ルール取得手段によって取得された上記ルールに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有するように構成される。

【0038】

このような画像形成装置では、ドキュメントに関する取り扱いのルールをドキュメント毎及び動作毎に管理する必要がなく、また、どのルールを適用すべきかを判断する必要がない。

【0039】

また、本発明は、請求項 17 に記載されるように、上記ルール取得手段は、上記外部サーバとの通信を Simple Object Access Protocol に従って制御する通信手段を有するように構成することができる。

【0040】

また、本発明は、請求項 18 に記載されるように、上記ルール取得手段は、上記外部サーバとの通信を制御する通信手段と、選択可能な機能の実行可否を示す実行可否情報を保持する選択機能保持手段と、上記選択機能保持手段によって保持される上記実行可否情報を参照することによって、上記ルールによって指定される上記動作を許可するために満たすべき動作要件を実行できるか否かを判断する動作要件判断手段とを有し、上記動作制御手段は、上記動作要件判断手段による判断結果に基づいて、上記ドキュメントに対する動作を制御するように構成することができる。

【0041】

また、上記第三の課題を解決するために、本発明は、請求項 19 に記載されるように、ネットワークを介して通信制御を行う通信手段と、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持する保持手段と、ドキュメント属性と上記ドキュメントに対して実行される動作とに基づいて、上記保持手段によって保持される上記セキュリティポリシーを参照し、該ドキュメントへの該動作に対する上記ルールを取得するポリシー取得手段とを有し、上記通信手段は、上記ネットワークを介して受信した上記ドキュメント属性と上記動作とを上記ポリシー取得手段に通知し、上記ポリシー取得手段が取得した上記ルールを送信するように構成される。

【0042】

このようなポリシー解釈サーバでは、ドキュメントに関する取り扱いのルールをドキュメント毎及び動作毎に管理する必要がない。

【0043】

また、本発明は、請求項 20 に記載されるように、上記ネットワークを介して接続される装置毎に選択可能な機能の実行可否を示す実行可否情報を保持する選択機能保持手段と、上記選択機能保持手段によって保持される上記実行可否情報を参照することによって、上記ポリシー取得手段によって取得した上記ルールによって指定される上記動作を許可するために満たすべき動作要件を実行可能か否かを判断する動作要件判断手段とを有するように構成することができる。

【発明の効果】

【0044】

本発明によれば、情報システムのセキュリティを確保するシステムに関し、特に、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う画像形成装置を提供することができる。

【0045】

また、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う装置にセキュリティポリシーを配布するポリシー配布サーバを提供することができる。

【0046】

更に、本発明は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいて、ネットワークを介して接続される装置に、該ドキュメントに対する動作を許可するための動作要件を提供するポリシー解釈サーバを提供することができる。

【発明を実施するための最良の形態】

【0047】

以下、本発明の実施の形態を図面に基づいて説明する。

【0048】

本発明の実施例を、以下に詳細に説明する。

【0049】

先ず、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーについ

て説明する。

【0050】

本実施例では、異なるタイプのシステムでドキュメントに対するセキュリティポリシーを共有するために、以下のような仕組みを使用して、セキュリティポリシーを記述する。ここでは、記述したセキュリティポリシーのことをドキュメントセキュリティポリシー（DSP）と呼ぶ。

【0051】

図1は、セキュリティポリシーの例を示す。ユーザの属する組織は、例えば、機密文書、丸秘文書、社外秘文書のような、文書の機密レベルごとに、ドキュメントに対して、例えば、図1のようなセキュリティポリシーを掲げることが想定される。

【0052】

このようなポリシーをDSPとして記述できるようにするために、以下のような方法を使用する。

【0053】

まず最初に、ドキュメントを機密レベル（極秘、丸秘、社外秘など）と、カテゴリー（人事文書、技術関連文書など）に応じて分類する。この、機密レベルとカテゴリーの組みを、ドキュメントのセキュリティラベルと呼ぶ。このセキュリティラベルは、実際には、個々のドキュメントに属性情報として付与される。

【0054】

上記のような、分類の仕方の一例を図2に示す。図2は、ドキュメントラベル用語ファイルの例を示す。図2に示されるようなドキュメントラベル用語ファイル300は、個々のドキュメントに属性情報として付与されるラベルのリストを管理するファイルであり、例えば、XMLによって記述される。

【0055】

DSPには、ドキュメントの機密レベル及びカテゴリーに応じて、ドキュメントに対して許可される操作（オペレーション）を規定し、そして、その操作を許可する際に実行されるべき要件（管理責任者の許可を得る、ラベルを印刷する、など）を指定できるようにする必要がある。そのような、ドキュメントの機密レベル及びカテゴリーを記述するのが、図2のドキュメントラベル用語ファイル300である。

【0056】

図2において、<enumeration>から</enumeration>で示される記述311及び記述321によって、2種類のカテゴリーが示される。

【0057】

記述311において、<enum_id>doc_category</enum_id>を示す記述312は、カテゴリーの識別情報が「doc_category」であることを示す。<enum_name>Document Category</enum_name>を示す記述313は、カテゴリーの名称が「Document Category」であることを示す。<description>文書カテゴリーの種類</description>を示す記述314は、このカテゴリーが何を分類するかを示す説明「文書カテゴリーの種類」を示す。

【0058】

<item>から</item>を示す記述315、記述316及び記述317によって、3つのカテゴリーの項目が示される。記述315は、<name>internal_doc</name>を示す記述によって、項目名が「internal_doc」であることを示し、<description>社内一般文書</description>を示す記述によって、その項目の説明「社内一般文書」を示す。

【0059】

記述316は、<name>human_resource_doc</name>を示す記述によって、項目名が「human_resource_doc」であることを示し、<description>人事関連文書</description>を示す記述によって、その項目の説明「人事関連文書」を示す。

【0060】

記述317は、<name>technical_doc</name>を示す記述によって、項目名が「technical_doc」であることを示し、<description>技術関連文書</description>を示す記述によっ

て、その項目の説明「技術関連文書」を示す。

【0061】

同様に、記述 3 2 1 において、<enum_id>doc_security_level</enum_id>を示す記述 3 2 2 は、カテゴリーの識別情報が「doc_security_level」であることを示す。<enum_name>Document Security Level</enum_name>を示す記述 3 2 3 は、カテゴリーの名称が「Document Security Level」であることを示す。<description>文書のセキュリティレベルの種類</description>を示す記述 3 2 4 は、このカテゴリーが何を分類するかを示す説明「文書のセキュリティレベルの種類」を示す。

【0062】

<item>から</item>を示す記述 3 2 5、記述 3 2 6 及び記述 3 2 7 によって、3 つのカテゴリーの項目が示される。記述 3 2 5 は、<name>basic</name>を示す記述によって、項目名が「basic」であることを示し、<description>社外秘</description>を示す記述によって、その項目の説明「社外秘」を示す。

【0063】

記述 3 2 6 は、<name>medium</name>を示す記述によって、項目名が「medium」であることを示し、<description>秘</description>を示す記述によって、その項目の説明「秘」を示す。

【0064】

記述 3 2 7 は、<name>high</name>を示す記述によって、項目名が「high」であることを示し、<description>極秘</description>を示す記述によって、その項目の説明「極秘」を示す。

【0065】

このように、ドキュメントラベル用語ファイル 3 0 0 によって、社内一般文書、人事関連文書及び技術関連文書のような、文書カテゴリーの種類が規定される。また、社外秘、秘、極秘のような、文書のセキュリティレベルの種類が規定される。

【0066】

図 3 から図 1 3 は、ポリシー用語ファイルの例を示す図を示す。図 3 から図 1 3 により、1 つのポリシー用語ファイル 4 0 0 を構成する。

【0067】

図 3 から図 1 3 に示されるようなポリシー用語ファイル 4 0 0 は、システムタイプの分類を記述し、そのシステムタイプごとに、オペレーションを列挙する。そして、そのオペレーションごとに、オペレーションの実行の際にサポート可能な要件を列挙しておく。ポリシー用語ファイル 4 0 0 は、例えば、XML によって記述される。

【0068】

図 3 において、列挙して記述する方法は、図 2 に示すドキュメントラベルファイル 3 0 0 での記述方法と同様に<enumeration>から</enumeration>までの記述を繰り返すことによって示される。<enumeration>から</enumeration>までの詳細な記述は、図 2 に示すドキュメントラベルファイル 3 0 0 での記述方法と同様であるので、ここでは、簡単な説明のみとする。

【0069】

例えば、図 3 においては、記述 4 1 1 によってシステムタイプが列挙される。記述 4 1 1 によると、「システムタイプの種類」として、「複写機」、「プリンタ」、「ファクシミリ」、「スキャナ」、「文書リポジトリ」、及び、「電子会議システム」が記述される。

【0070】

そして、例えば、図 4 に示されたように、記述 4 2 1 から記述 4 7 1 によってシステムタイプごとの各オペレーションが列挙される。

【0071】

記述 4 2 1 において、「複写機に関わるオペレーション」として、「紙から紙への複写」が記述される。記述 4 3 1 において、「プリンタに係わるオペレーション」として、「

電子文書を紙へ印刷」が記載される。記述 4 4 1 において、「ファックスに関わるオペレーション」として、「ファックス送信」及び「ファックス受信」が記載される。記述 4 5 1 において、「スキャナに関わるオペレーション」として、「紙文書をスキャンして電子文書にする」が記載される。

【 0 0 7 2 】

記述 4 6 1 において、「文書リポジトリに関わるオペレーション」として、「保存する」、「改訂・編集する」、「削除・破棄する」、「参照する」、「ネットワークで配布する（送信する）」、「ディスクで配布する（送付する）」、及び、「アーカイブ・バックアップする」が記述される。記述 4 7 1 において、「電子会議システムに関わるオペレーション」として、「会議で利用する」が記述される。

【 0 0 7 3 】

更に、例えば、図 6 から図 1 3 示すように、記述 4 8 1 から記述 6 0 1 によってオペレーション毎に適用できる要件が列挙される。

【 0 0 7 4 】

記述 4 8 1 において、「複写に関わる要件」として、「明示的な許可」、「監査証跡の記録」、及び、「監査証跡のイメージ付き記録」が記載される。

【 0 0 7 5 】

記述 4 9 1 において、「印刷に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「プリントした本人による紙出力」、「信頼チャネルの利用（印刷データの暗号化）」、及び、「プリントアウトに追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【 0 0 7 6 】

記述 5 0 1 において、「ファックス送信に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「宛先制限」、「親展モードでの送信」、「信頼チャネルの利用」、「送信ファックスに追跡情報埋め込み（透かし、ラベル、バーコード）」、及び、「否認防止（受取証の取得）」が記載される。

【 0 0 7 7 】

記述 5 1 1 において、「ファックス受信に関わる要件」として、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「親展ファックスの宛先本人による取り出し」、「信頼タイムスタンプ」、及び、「受信ファックスに追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【 0 0 7 8 】

記述 5 2 1 において、「スキャンに関わる要件（保存した後については保存要件を適用する）」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、及び、「スキャン画像に追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【 0 0 7 9 】

記述 5 3 1 において、「保存に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「保存データの暗号化」、及び、「保存データの改ざん保護」が記載される。

【 0 0 8 0 】

記述 5 4 1 において、「改訂に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、及び、「バージョン管理」が記載される。

【 0 0 8 1 】

記述 5 5 1 において、「削除・破棄に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、及び、「完全消去」が記載される。

【 0 0 8 2 】

記述 5 6 1 において、「参照に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「編集禁止のデータのみ参照許可」、「印刷禁止のデータのみ参照

許可」、「参照場所限定のデータのみ参照許可」、及び、「ユーザ限定のデータのみ参照許可」が記載される。

【0083】

記述 5 7 1 において、「ネットワーク配信（送信）に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「信頼チャンネルの利用（送信データの暗号化）」、「宛先制限（社内のみ配信可能など）」、「編集禁止のデータのみ配信許可」、「印刷禁止のみ配信許可」、「参照場所限定のデータのみ配信許可」、及び、「ユーザ限定のデータのみ配信許可」が記載される。

【0084】

記述 5 8 1 において、「ディスク配布（送付）に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「送付データの暗号化」、「送付データの改ざん保護」、「編集禁止のデータのみ送付許可」、「印刷禁止のみ送付許可」、「参照場所限定のデータのみ送付許可」、及び、「ユーザ限定のデータのみ送付許可」が記載される。

【0085】

記述 5 9 1 において、「アーカイブ・バックアップに関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「アーカイブデータの暗号化」、及び、「アーカイブデータの改ざん保護」が記載される。

【0086】

記述 6 0 1 において、「会議での利用に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、及び、「監査証跡のイメージ付き記録」が記載される。

【0087】

図 2 のドキュメントラベル用語ファイルと図 3 から図 1 3 のポリシー用語ファイルとに基づく DSP について図 1 4 から図 2 2 で説明する。図 1 4 から図 2 2 は、ポリシーファイルの例を示す図である。上述の図 2 に示すドキュメントラベル用語ファイル 3 0 0 と、図 3 から図 1 3 のポリシー用語ファイル 4 0 0 とに基づいて、ユーザの組織内でのセキュリティに対するポリシーが、例えば図 1 4 から図 2 2 に示す DSP 2 0 0 0 のように XML で記述され、1 つのポリシーファイルを構成する。

【0088】

図 1 4 から図 2 2 に示されるような DSP 2 0 0 0 は、<policy>で示される記述 2 0 0 1 から</policy>で示される記述 2 0 0 2 にてポリシーが示される。

【0089】

図 1 4 の<acc_rule>を示す記述 2 0 1 1 から図 1 6 の</acc_rule>を示す記述 2 0 1 2 において、<doc_category>ANY</doc_category>及び<doc_security_level>basic</doc_security_level>を示す記述 2 0 1 3 によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「basic（基本レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>ANY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述 2 0 1 7 によって、ユーザカテゴリ「ANY（非限定）」かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【0090】

図 1 6 の<acc_rule>を示す記述 2 0 2 1 から図 1 9 の</acc_rule>を示す記述 2 0 2 2 において、<doc_category>ANY</doc_category>及び<doc_security_level>medium</doc_security_level>を示す記述 2 0 2 3 によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「medium（中レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>DOC-CATEGORY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述 2 0 2 7 によって、ユーザカテ

リ「DOC-CATEGORY（文書カテゴリーの種類）」（図2の記述312、313及び314参照）かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【0091】

また、同様のドキュメント属性を有するドキュメントに対して、図18の<user_category>ANY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述2028によって、ユーザカテゴリ「ANY（非限定）」かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【0092】

図19の<acc_rule>を示す記述2031から図19の</acc_rule>を示す記述2032において、<doc_category>ANY</doc_category>及び<doc_security_level>high</doc_security_level>を示す記述2023によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「high（高レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>DOC-CATEGORY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述2037によって、ユーザカテゴリ「DOC-CATEGORY（文書カテゴリーの種類）」（図2の記述312、313及び314参照）かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【0093】

次に、図14から図22のDSP2000の構造を、図23から図25を参照して、以下に、詳しく説明する。

【0094】

図23は、DSPの識別情報の例を示す図である。DSP2000の識別情報210において、<about_this_policy>と</about_this_policy>とで囲まれた範囲の記述211～213には、DSP2000を識別するための識別情報が記述される。

【0095】

<serial_number>RDSP2023</serial_number>を示す記述211には、DSP2000を他のDSPと区別するためのシリアル番号が記述される。

【0096】

<terminology_applied>RDST9487</terminology_applied>で示される記述212には、DSP2000に対応するポリシー用語ファイル400のシリアル番号が記述される。尚、この定義ファイルは更新される可能性があるため、このDSP2000がどのポリシー用語ファイルに基づいて記述されているのかを明確にするために記録しておく。記述213には、<title>DOCUMENT-SECURITY-POLICY</title>を示す記述によってDSP2000のタイトル、<version>1.20</version>を示す記述によってバージョン番号、<creation_date>2002/02/18 22:30:24</creation_date>を示す記述によって作成日時、<creator>Taro Tokyo</creator>を示す記述によって作成者、<description>sample document security policy.</description>を示す記述によって説明などの一般的な書誌情報が記述される。

【0097】

そして、DSP2000の識別情報は、</about_this_policy>により終了する。

【0098】

次に、上述の D S P 2 0 0 の識別情報に続いて、ポリシーの内容を<policy>と</policy>で囲まれた範囲に記述する。図 2 4 は、D S P の構造を説明するための記述例を示す図である。

【0 0 9 9】

図 2 4 に示されるポリシーの内容 2 2 0 は、以下に説明するように、階層構造を用いて記録する。

【0 1 0 0】

ポリシー<policy>は、複数のアクセス制御ルール<acc_rule>（記述 2 2 1）で構成される。一つのアクセス制御ルール<acc_rule>（記述 2 2 1）は、対象とするドキュメントのカテゴリ<doc_category>とレベル<doc_security_level>を一意に指定し（記述 2 2 2）、さらにアクセス制御リスト<acl>（記述 2 2 3）を一つ含むように構成される。

【0 1 0 1】

アクセス制御リスト<acl>（記述 2 2 3）は、複数のアクセス制御エレメント<ace>（記述 2 2 4）で構成される。

【0 1 0 2】

各アクセス制御エレメント<ace>（記述 2 2 4）は、対象とするユーザのカテゴリ<user_category>（記述 2 2 5）とレベル<user_security_level>（記述 2 2 6）を一意に指定し、さらに複数のオペレーション<operation>（記述 2 2 7）で構成される。

【0 1 0 3】

各<operation>（記述 2 2 7）は、一つのオペレーション名<name>（記述 2 2 8）と、一つの禁止<denied/>（記述 2 2 9）、または一つの許可<allowed/>（記述 2 3 2）、または複数の<requirement>（記述 2 3 0 及び記述 2 3 1）で構成される。

【0 1 0 4】

記述 2 2 2 において、ドキュメントのカテゴリ<doc_category>やユーザのカテゴリ<user_category_level>に記述している” ANY” は、どのカテゴリ、及び、レベルにも適用されることを示している。また、記述 2 2 5 によって示されるユーザのカテゴリ<user_category>の” DOC-CATEGORY” は、ユーザのカテゴリがドキュメントのカテゴリと同じときに適用されることを示している。

【0 1 0 5】

この実施例では、禁止するオペレーションには<denied/>（記述 2 2 9）を指定するようにしているが、D S P 2 0 0 0 に記載されていなければアクセスは許可されていないことを表している、というように構成してもよい。

【0 1 0 6】

このように、D S P を記述することにより、ドキュメントのタイプ（カテゴリ、レベル）に応じて、どのようなユーザタイプ（カテゴリ、レベル）が、ドキュメントに対してどのようなオペレーションが可能なのかを記述できる。そして更に、そのドキュメントについて、ユーザが、オペレーションが可能の場合には、どのような要件を満たさなければならないのかを明確に記述することができる。

【0 1 0 7】

そして、D S P を、上記のようにプラットフォームに依存しないXMLで記述することにより、異なるタイプのシステム間で、このD S P を共通に利用することができる。特に、セキュリティポリシーを適用したい対象は、電子的なドキュメントに限らず、紙のドキュメントに対しても適用できなければならないため、図 3 から図 1 3 のドキュメントラベルファイルや図 1 4 から図 2 2 のD S P 2 0 0 0 に記述しているように、紙ドキュメントに関するオペレーション（hardcopy, scanなど）も規定できる。

【0 1 0 8】

本実施例の、図 2 4 に示す要件の中に、以下の<requirement>explicit_authorization</requirement>を示す記述 2 3 1 が存在する。これは、「ドキュメントの管理責任者により明示的な許可が得られた場合には、そのオペレーションを許可する」という要件である。すべて、このD S P に従ってオペレーションがコントロールされるようになると、自由

度が無くなる恐れが生じる。しかし、この明示的な許可という要件を指定できるようにすることにより、柔軟なオペレーションコントロールが可能となる。

【0109】

また、本実施例の特徴として、その「明示的な許可」という要件を指定可能にすることによって、明示的な許可が得られれば実行してもよいオペレーションと、明示的な許可が得られたとしても禁止しなければならないオペレーションとを区別することができるということである。

【0110】

従って、DSPに記載しないか又は、<denied/>で指定されたオペレーションは明示的な許可が得られたとしても禁止しなければならないオペレーションである。これにより、ポリシーを記述している側の意図を、的確に規定できるようになり、誤って許可を与えてしまつてオペレーションが実行されてしまうというような事態をあらかじめ防ぐように規定することができる。

【0111】

次に本発明のDSPの別の記述形を図26で説明する。図25は、DSPの他の記述例を示す図である。図26に示すポリシーの内容240は、無条件で許可するオペレーションや、禁止するオペレーションが多くなった場合には、オペレーションごとに<operation><allowed/></operation>というような入れ子構造を記述するのは効率が悪いので、無条件で許可するオペレーションを列挙する、<allowed_operations>を示す記述243と、許可しないオペレーションを列挙する、<denied_operations>を示す記述241を使用するようにしても良い。

【0112】

また、<requirement>explicit_authorization</requirement>を示す記述242は、図24での説明と同様である。

【0113】

図26は、上述のDSPを蓄積し且つ配布する種々の媒体を示す。

【0114】

以上で説明したように、図26に示されたDSP2000は、XML (Extensible Markup Language) で記述されている。そして、電子的なファイルとして記録しておくことができる。また、その電子的なファイルを格納した、例えば、ハードディスク51、光磁気ディスク52、フレキシブルディスク53、又は、CD-ROM、CD-R、CD-RW、DVD、DVD-R、DVD-RAM、DVD-RW、DVD+RW、DVD+Rのような光ディスク54のような記憶媒体を作成することができる。また、その電子的なDSP2000をコンピュータ55を使用して、ネットワーク56を介してで伝送することができる。

【0115】

このDSP2000は、特定のシステム向けのセキュリティポリシーの記述ではなく、異なる複数のシステムで共通に利用できるセキュリティポリシーの記述である。従って、このセキュリティポリシー記述を記憶した記憶媒体を作成し、そして配布したり又は、ネットワーク経由して伝送したりすることにより、複数のシステムで共通に利用しやすくなる。

【0116】

図27は、本発明の一実施例に係る画像形成装置のハードウェア構成を示すブロック図である。図27において、画像形成装置1000は、コンピュータによって制御される装置であつて、CPU (中央処理装置) 11と、ROM (Read-Only Memory) 12と、RAM (Random Access Memory) 13と、不揮発性RAM (non-volatile Random Access Memory) 14と、リアルタイムクロック15、イーサネット (登録商標) I/F (Ethernet (登録商標) Interface) 21と、USB (Universal Serial Bus) 22と、IEEE (Institute of Electrical and Electronics Engineers) 1284 23と、ハードディスク I/F 24と、エンジン I/F 25と、RS-232C I/F 26と、ドライバ27とで

構成され、システムバスBに接続される。

【0117】

CPU11は、ROM12に格納されたプログラムに従って画像形成装置1000を制御する。RAM13には、例えば、各インターフェース21から26に接続される資源に領域が割り当てられる。不揮発性RAM14には、画像形成装置1000を制御するためにCPU11による処理で必要な情報が格納される。リアルタイムクロック15は、現時刻を計ると共に、処理を同期させる場合にCPU11によって使用される。

【0118】

イーサネット（登録商標）I/F21には、10BASE-T又は100BASE-TX等のイーサネット（登録商標）用インターフェースケーブルが接続される。USB22には、USB用インターフェースケーブルが接続される。IEEE1284 23には、IEEE1284用インターフェースケーブルが接続される。

【0119】

ハードディスクI/F24には、ハードディスク34が接続され、ネットワークを介して送信された印刷すべき文書の文書データ、又は、印刷処理後の画像データがハードディスクI/F24を介してハードディスク34に格納される。エンジンI/F25には、文書データに基づいて所定媒体に印刷を行うプロッタ35-1及び画像データを取り込むスキャナ35-2等が接続される。RS-232C I/F26には、オペレーションパネル36が接続され、ユーザへの情報の表示及びユーザから入力情報又は設定情報の取得が行われる。

【0120】

画像形成装置1000によって行われる処理を実現するプログラムは、例えば、CD-ROM等の記憶媒体37によって画像形成装置1000に提供される。即ち、プログラムが保存された記憶媒体37がドライバ27にセットされると、ドライバ27が記憶媒体37からプログラムを読み出し、その読み出されたプログラムがシステムバスBを介してハードディスク34にインストールされる。そして、プログラムが起動されると、ハードディスク34にインストールされたプログラムに従ってCPU11がその処理を開始する。尚、プログラムを格納する記憶媒体37としてCD-ROMに限定するものではなく、コンピュータが読み取り可能な記憶媒体であればよい。プログラムをネットワークを介してダウンロードし、ハードディスク34にインストールするようにしても良い。

【0121】

セキュリティポリシーに従って動作する画像形成装置について図28、図29及び図30を参照して以下に詳細に説明する。

【0122】

図28は、セキュリティポリシーに従って動作する読み取り装置としての画像形成装置の機能構成を示す図である。

【0123】

図28に示す読み取り装置としての画像形成装置1000は、主に、読み取り部71と、読み取り条件取得部72と、データ送信先取得部73と、データ処理部74と、データ送信部75と、ポリシー実行部1001と、読み取り画像データ61と、蓄積データ62とを有する。

【0124】

また、ポリシー実行部1001は、ドキュメント属性取得部1011と、動作要件選択部1012と、動作制御部1013と、ユーザ属性取得部1021とを有する。ドキュメント属性取得部1011は紙原稿60から又は読み取り画像データ61からドキュメント属性を取得して、動作要件選択部1012へ通知する。

【0125】

一方、ユーザ属性取得部1021は、ユーザによって入力されたユーザ情報を取得すると、動作要件選択部1012に通知する。動作要件選択部1012は、DSP2000に従って許可される場合の要件を選択し、その結果を動作制御部1013に通知する。動作

制御部 1013 は、読み取った紙原稿 60 の画像データに対するデータ処理を指示する。

【0126】

ポリシー実行部 1001 において、点線で示される部分について省略しても良い。

【0127】

読み取り部 71 は、読み取り条件取得部 72 から通知されるユーザによって入力された読み取り条件に従って、紙原稿 60 を読み取る（スキャン）する処理部であり、読み取った画像データは、読み取り画像データ 61 に格納される。また、画像データ 61 から取得したドキュメント属性をドキュメント属性取得部 1011 に通知する。

【0128】

読み取り条件取得部 72 は、ユーザによって入力された読み取り条件を取得し、読み取り部 71 とデータ処理部 74 とへ通知する。

【0129】

データ送信先取得部 73 は、ユーザによって入力されたデータ送信先を取得し、データ送信部 75 に通知する処理部である。

【0130】

データ処理部 74 は、動作制御部 1013 から提供される要件を満たすように読み取り条件取得部 72 から通知されるユーザによって入力された読み取り条件に従って、データ処理を読み取った画像データに行い、データ処理された画像データを蓄積データ 62 に蓄積する。

【0131】

データ送信部 75 は、動作制御部 1013 から通知される要件を満たすように、蓄積データ 62 から取り出した処理対象となる画像データをデータ送信先取得部 73 から通知された送信先へ送信する。

【0132】

画像データを外部に送信する必要がある場合、データ送信部 28 を省略しても良い。また、画像データを記憶媒体 37 に記憶するようにしても良い。

【0133】

図 28 において、読み取り装置としての画像形成装置 1000 は、専用のハードウェアにより構成するように記載されているが、汎用のコンピュータとそのコンピュータ上で実行されるプログラムにより構成されても良い。

【0134】

また、以下に説明する本発明の実施例をコンピュータ上で実行するプログラムは、コンピュータにより読み出し可能な記憶媒体に記録され、その実行前に、コンピュータにより読み込まれる。また、このようなプログラムは、コンピュータネットワークを介して配信されることも可能である。

【0135】

図 29 は、簡略化した DSP の例を示す図である。説明の便宜のため、DSP 2000 を簡略化した DSP で説明する。図 29 に示される DSP 2100 において、つぎのようにルール 1 からルール 3 を示す。

【0136】

ルール 1 は、図 29 の第 4 行目の<acc_rule>から、第 10 行目の<user_security_level>ANY</user_security_level>までの部分及び、第 11 行目<operation>から、第 14 行目</operation>までの部分により記述される。

【0137】

第 5 行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわらずルール 1 が適用されることを示す。

【0138】

第 6 行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルが basic のときを示す。

【0139】

第9行目の<user_category>ANY</user_category>は、ユーザのカテゴリにかかわらないことを示す。

【0140】

第10行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわらないことを示す。

【0141】

更に第12行目と第13行目の<name>scan</name>及び<allowed/>は、読み取りは要件なく許可されることを示す。

【0142】

従って、ルール1では、第5行目、第6行目、第9行目、第10行目、第12行目及び第13行目により、文書カテゴリにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは要件なく許可される。

【0143】

次に、ルール2は、図29の第4行目の<acc_rule>から、第10行目の<user_security_level>ANY</user_security_level>までの部分及び、第15行目<operation>から、第20行目</operation>までの部分により記述される。

【0144】

第5行目の<doc_category>ANY</doc_category>は、文書カテゴリにかかわりなくルール2が適用されることを示している。

【0145】

第6行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【0146】

第9行目の<user_category>ANY</user_category>は、ユーザのカテゴリにかかわらないことを示す。

【0147】

第10行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわらないことを示す。

【0148】

更に、第16行目から第19行目の

<name>net_delivery</name>

<requirement>audit</requirement>

<requirement>print_restriction</requirement>

<requirement>trusted_channel</requirement>

は、ネットワーク配信は、「ログを記録すること」と、「プリント制限をかけること」、「信頼できるチャネルを使用すること」の要件を満たすときに許可されることを示す。

【0149】

従って、ルール2では、第5行目、第6行目、第9行目、第10行目、第16行目から第19行目により、文書カテゴリにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、ネットワーク配信は、ログを記録することと、プリント制限をかけること、信頼できるチャネルを使用することの要件を満たすときに許可されることを示している。

【0150】

そして、ルール3は、図29の第24行目の<acc_rule>から、第30行目の<user_security_level>ANY</user_security_level>までの部分及び、第31行目<operation>から、第35行目</operation>までの部分により記述される。

【0151】

第25行目の<doc_category>ANY</doc_category>は、文書カテゴリにかかわりないこ

とを示す。

【0152】

第26行目の<doc_security_level>high</doc_security_level>は、文書のセキュリティレベルがhighの場合を示す。

【0153】

第29行目の<user_category>DOC-CATEGORY</user_category>は、ユーザのカテゴリが文書のカテゴリと同じであることを示す。

【0154】

第30行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわらずを示す。

【0155】

第32行目から第34行目の、

<name>scan</name>

<requirement>audit</requirement>

<requirement>embed_trace_info</requirement>

は、読み取りは、「ログを記録すること」及び、「追跡可能な情報を埋め込むこと」の要件を満たすときに許可される。

【0156】

従って、ルール3では、第25行目、第26行目、第29行目、第30行目、第31行目から第34行目により、文書カテゴリにかかわらず、文書のセキュリティレベルが”high”の場合には、ユーザのカテゴリが文書のカテゴリと同じであり、且つ、ユーザのセキュリティレベルにかかわらず、読み取りは、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可されることを示している。

【0157】

ここで、「追跡可能な情報を埋め込むこと」には、例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加などを含んでも良い。また、表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。さらに、「ログを記録すること」には、読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。また、「ログを記録すること」には、ネットワーク配信を指示したユーザの認証データとネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。

【0158】

図28を参照しつつ、詳細な動作について説明する。

【0159】

上述の図29に示すDSP2100に基づいて、例えば、セキュリティレベルが”basic”の文書を読み取りしようとしている場合には、抽出すべき要件はない。

【0160】

また、上述の図29に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、前述のように、「ログを記録すること」及び「追跡可能な情報を埋め込むこと」が、読み取りの要件となる。「ログを記録すること」及び「追跡可能な情報を埋め込むこと」の内容に関しては、上述と同様である。

【0161】

次に、セキュリティレベルが”basic”のときの場合のように、抽出すべき要件がない場合には、動作制御部1013は、データ処理部71に対して、文書の読み取りを指示し、ユーザは文書データを取得して終了する。

【0162】

一方、セキュリティレベルが”high”のときの場合のように、抽出すべき要件がある場

合には、動作要件選択部 1 0 1 2 は、その要件をすべて満たすことができるかを判定し、その判断結果を動作制御部 1 0 1 3 に通知する。

【0 1 6 3】

動作要件選択部 1 0 1 2 による判断結果がすべての要件を満たすことができないことを示す場合は、動作制御部 1 0 1 3 は、データ処理部 7 4 に対してデータ処理を禁止するように指示し、データ処理部 7 4 は読み取りデータを破棄して終了する。ユーザに対してはデータ処理が行えないことを通知する。

【0 1 6 4】

一方、動作要件選択部 1 0 1 2 による判断結果がすべての要件を満たすことができることを示す場合は、動作制御部 1 0 1 3 データ処理部 7 4 に対して、その要件を満たすようにデータ処理を行うように指示する。ユーザは文書データを取得して終了する。

【0 1 6 5】

この場合には、以下の処理が実行される。

【0 1 6 6】

ユーザ属性取得部 1 0 2 1 は、オペレーションパネル 3 6 から読み取り指示を出したユーザに、ユーザ ID の入力要求を出す。ユーザは、オペレーションパネル 3 6 からユーザ ID を入力する。ユーザ属性取得部 1 0 2 1 は、ユーザ ID からデータベース 1 0 2 に登録されている入力されたユーザ ID に対応するカテゴリー、セキュリティレベルを取得し、動作要件選択部 1 0 2 1 に通知する。

【0 1 6 7】

ログを記録する場合、読み取った文書データに追跡可能な情報の埋め込み(例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)を行う。表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。

【0 1 6 8】

最後に、ユーザは紙原稿 6 0 の画像データを蓄積データ 6 2 内に取得して終了する。

【0 1 6 9】

以上のように、図 2 9 に示したセキュリティポリシーに従って、紙原稿 (ドキュメント) 6 0 を読み取ることができる。

【0 1 7 0】

次に、画像形成装置 1 0 0 0 が紙原稿 6 0 を読み取り且つ読み取った文書をネットワークに配信する場合について説明する。

【0 1 7 1】

まず、ユーザが、画像形成装置 1 0 0 0 に紙原稿 6 0 をセットし、オペレーションパネル 3 6 から、読み取り条件の入力、読み取りデータの配信先の指定及び紙原稿 6 0 の読み取り指示を出す。

【0 1 7 2】

読み取り部 7 1 が、紙文書の読み取りを行う。ドキュメント属性取得部 1 0 1 1 は、読み取った紙原稿 6 0 の画像データのバーコードや電子透かしなどの画像情報から文書 ID を抽出し、カテゴリー、セキュリティレベルを取得して、動作要件選択部 1 0 1 2 に通知する。

【0 1 7 3】

動作要件選択部 1 0 1 2 は、ドキュメント属性取得部 1 0 1 1 が通知したドキュメント属性に従って、DSP 2 1 0 0 中の対応するエントリを検索し、要件を抽出する。

【0 1 7 4】

上述の図 2 9 に示す DSP 2 1 0 0 に基づいて、例えば、セキュリティレベルが "basic" の文書を読み取り、ネットワーク配信しようとしている場合には、読み取りに関する要件はない。しかし、上述のように、ネットワークに配信する時には、「ログを記録すること」と「プリント制限をかけること」と「信頼できるチャネルを使用すること」が要件となる。

【0175】

また、上述の図29に示すDSP2100に基づいて、例えば、セキュリティレベルが” high”の文書を読み取りしようとしている場合には、読み取りに関する要件として、「ログを記録すること」と「追跡可能な情報を埋め込むこと(例えば、上述のような、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)」が要件となる。しかし、ネットワークに配信することを許可するルールがないため、許可されない。

【0176】

例えば、ドキュメントをネットワークへ配信する際の要件が、DSP2100内に存在しない場合には、動作制御部1013は、データ送信部75に対して配信の指示を行い、ドキュメントをネットワークへ配信して、処理を終了する。

【0177】

一方、例えば、ドキュメントをネットワークへ配信する際の要件が、DSP2100内に存在する場合には、動作要件選択部1012が、その要件をすべて満たすことができるかを判定する。

【0178】

ネットワークに配信することを許可するルールがない場合には、動作制御部1013が、ユーザに、「ネットワークに配信することを許可するルールがない」ことを通知をして、紙原稿60の画像データを破棄して終了する。例えば、セキュリティレベルが” high”の場合である。

【0179】

動作要件選択部1012によってすべての要件を満たすことができないと判断した場合は、動作制御部1013が、ユーザに通知をして、データ処理部74に対して紙原稿60の画像データを破棄するように指示して終了する。

【0180】

例えば、上述のセキュリティレベルが” basic”の場合のように、すべての要件を満たすことができる場合は、動作制御部1013は、その要件を満たした読み取りをデータ処理部74に指示し、また、データ送信部75にドキュメントをネットワークに配信するように指示して終了する。

【0181】

そして、ユーザ属性取得部1012は、オペレーションパネル36から読み取り指示を出したユーザに、ユーザIDの入力要求を出す。

【0182】

ユーザが、オペレーションパネル36からユーザIDを入力すると、ユーザ属性取得部1021は、ユーザIDに対応するカテゴリー、セキュリティレベルを取得し、動作要件選択部1012に通知する。動作制御部1013は、動作要件選択部1012から通知される要件に従ってログを記録する。

【0183】

更に、動作制御部1013は、データ処理部74に対して、読み取った紙原稿60の画像データを、印刷不可能なデータ(たとえばADOBE(登録商標)の印刷禁止属性を持ったPDFなど)に変換するように指示を行う。

【0184】

最後に、動作制御部1013は、データ送信部75に対して配信指示を行い、データ送信部75は、信頼できる通信経路(たとえばIPsecやVPNなど)を通じて、ドキュメントをネットワークへ配信し、終了する。

【0185】

以上のように、図29に示したDSP2100を使用して、図28に示した文書読み取り装置としての画像形成装置1000が、文書を読み取り且つ読み取った文書をネットワークに配信することができる。

【0186】

セキュリティポリシーに従った動作を実現する複写装置としての画像形成装置の機能構成について図30で説明する。図30は、セキュリティポリシーに従って動作する複写装置としての画像形成装置の機能構成を示す図である。図30中、図28と同様の処理部には同一符号を付しその詳細な説明を省略する。

【0187】

図30において、複写装置としての画像形成装置1000-2は、図28に示す画像形成装置1000の読み取り条件取得部72及びデータ送信先取得部73の代わりに複写条件取得部81と、図28に示す画像形成装置1000のデータ送信部75の代わりに印刷部82とを有する点において、図28に示す画像形成装置1000と異なっている。

【0188】

しかしながら、画像形成装置1000が画像形成装置1000-2の複写条件取得部81と、印刷部82とを更に有するように構成しても良い。点線で示される部分1002は省略しても良い。

【0189】

複写条件取得部81は、ユーザがオペレーションパネル36に入力した複写条件を取得して、読み取り部71とデータ処理部74とへ複写条件を通知すると共に、印刷部82へも通知する。

【0190】

印刷部82は、動作制御部1013からの指示に応じて、蓄積データ62から紙原稿60の画像データを取得し、動作制御部1013から通知された要件を満たすように複写条件取得部81から通知されて複写条件に従って印刷処理を行い、用紙に画像データが形成された複写原稿60bを出力する。

【0191】

以下に、外部から画像形成装置1000又は1000-2に対してポリシーを設定する方法について説明する。例えば、ポリシーとして図14から図22に記載されるDSP2000が配布される。ポリシーとしてDSP2000が、外部サーバから画像形成装置1000又は1000-2へ配布される際には、SOAP(Simple Object Access Protocol)に従った通信によって行われる。

【0192】

図31から図44に示される画像形成装置1000又は1000-2は、読み取り装置又は複写装置としての画像形成装置に限定されず、読み取り機能と複写機能とを有する、或いは、それ以上の(例えば、スキャナ、コピー、FAX、プリンタ等)複数の異なる画像形成処理を可能とする画像形成装置であっても良い。

【0193】

先ず、画像形成装置1000又は1000-2が一方的に送り付けられるポリシーを受信する第一のポリシー設定方法について図31で説明する。

【0194】

図31は、外部サーバからポリシーが配布される第一のポリシー設定方法を示す図である。図31において、ポリシーを設定しようとする管理者が使用する管理者コンソール4001と、外部サーバとしてポリシーを配布するポリシー配布サーバ4000と、画像形成装置1000又は1000-2とがネットワーク5を介して接続される。ポリシー配布サーバ4000は、サーバコンピュータであって、SOAPクライアント機能4021を有し、画像形成装置1000は、SOAPサーバ機能4022を有する。図31中、画像形成装置1000又は1000-2を画像形成装置1000として説明する。

【0195】

図31に示す第一のポリシー設定方法では、管理者が管理者コンソール4001からポリシーとしてDSP2000をポリシー配布サーバ4000に送信する(ステップS11)。そして、ポリシー配布サーバ4000がSOAPクライアント機能4021を利用して、ポリシーとしてDSP2000を配布し(ステップS12)、画像形成装置1000は、SOAPサーバ機能4022でDSP2000をポリシーとして受信し、受信結果を

返す。

【0196】

そして、画像形成装置1000は、配布されたDSP2000に従って、動作要件の選択を行い、動作要件を満たすように動作する（ステップS13）。

【0197】

このような構成の場合に、画像形成装置1000は、ポリシーを送信するポリシー配布サーバ4000が信頼できるものであるか否かを確認することで、間違ったポリシーの受信や悪意あるポリシーの設定などを防ぐこともできる。すなわち、ポリシー配布サーバ4000がポリシーの配布をする時に、以下のような動作を実行する。

【0198】

上記ステップS12において、ポリシー配布サーバ4000は、自分自身の認証情報とポリシーとしてDSP2000を画像形成装置1000に送信する。

【0199】

次に、画像形成装置1000は、送信されたポリシー配布サーバ4000の認証情報を検証する（ステップS12-2）。

【0200】

そして、このポリシー配布サービス4000の認証情報が正しいと確認された場合、画像形成装置1000は、ポリシーとして送信されたDSP2000を正式なものとし、配布されたDSP2000に従って、動作要件の選択を行い、動作要件を満たすように動作する（ステップS13）。

【0201】

このようなポリシー配布サーバ4000の認証を行うことによって、画像形成装置1000は、間違ったポリシーの受信や悪意あるポリシーの設定を防ぐことができる。

【0202】

次に、画像形成装置1000又は1000-2が、ポリシー配布サーバ4000からポリシーの配布通知を受けてポリシーを取得しにいく第二のポリシー設定方法について図32で説明する。

【0203】

図32は、外部サーバからポリシーを取得する第二のポリシー設定方法を示す図である。図32において、図31と同様に、管理者コンソール4001と、ポリシー配布サーバ4000と、画像形成装置1000又は1000-2とがネットワーク5を介して接続される。ポリシー配布サーバ4000は、SOAPクライアント機能4021とSOAPサーバ機能2024とを有し、画像形成装置1000又は1000-2は、SOAPサーバ機能4022とSOAPクライアント機能4023とを有する。図32中、画像形成装置1000又は1000-2を画像形成装置1000として説明する。

【0204】

図32に示す第二のポリシー設定方法では、管理者が管理者コンソール4001からポリシーとしてDSP2000をポリシー配布サーバ4000に送信する（ステップS21）。そして、ポリシー配布サーバ4000がSOAPクライアント機能4020を利用して、ポリシーとしてDSP2000の配布があったことを通知し（ステップS22）、画像形成装置1000は、SOAPサーバ機能4022でその配布通知を受信し、受信結果を返す。

【0205】

その後、画像形成装置1000は、SOAPクライアント機能4023を利用して、ポリシー取得要求を送信すると、ポリシー配布サーバ4000は、SOAPサーバ機能2024でそのポリシー取得要求を受信して、受信結果としてポリシー（管理者コンソール4001から受信したDSP2000）を送信する（ステップS23）。

【0206】

そして、画像形成装置1000は、配布されたDSP2000に従って、動作要件の選択を行い、動作要件を満たすように動作する（ステップS24）。

【0207】

ステップS22にて、ポリシー配布サーバ4000は、画像形成装置1000にDSP2000を識別する識別情報を送信することによってポリシー配布通知を行うようにしても良い。この場合、ステップS23において、画像形成装置1000は、ポリシー配布サーバ4000から受信した識別情報を送信することによってポリシー取得要求を行うようにすれば良い。

【0208】

更に、このような場合には、ポリシーを受信する画像形成装置1000が信頼できるものであるか否かを確かめることで情報の漏洩（ここではポリシー）を防ぐことができる。即ち、画像形成装置がポリシー配布サーバ4000からポリシーを取得する際に以下のような動作を実行する。

【0209】

先ず、上記ステップS23において、画像形成装置1000は、自分自身の認証情報をポリシー取得要求に付加して、ポリシー配布サーバ4000に送信する。

【0210】

次に、ポリシー配布サーバ4000は、画像形成装置1000から受信した認証情報を検証する（ステップS23-2）。そして、ポリシー配布サーバ4000は、画像形成装置1000の認証情報が正しいと確認した場合、ポリシーとしてDSP2000を画像形成装置1000へ送信する（ステップS23-4）。

【0211】

このような画像形成装置1000の認証を行うことによって、ポリシー配布サーバ4000は、情報の漏洩（ここではポリシー）を防ぐことができる。

【0212】

第二のポリシー設定方法は、画像形成装置1000が比較的容量のあるポリシーを次々に受信すると記憶領域が不足してしまうような場合に、画像形成装置1000が必要な時にポリシーを取得するようにすることができる点で有効である。

【0213】

この第二のポリシー設定方法において、画像形成装置1000は、配布通知を受けて速やかにポリシー取得要求を行っても良いし、配布通知を受けたことを装置内部に記憶しておいて、所定のタイミングでポリシー取得要求を行っても良い。

【0214】

所定のタイミングでポリシー取得要求を行うポリシー設定方法の変形例について図33、図34及び図35について説明する。

【0215】

図33は、電源投入時にポリシーを取得する第三のポリシー設定方法を示す図である。図33中、画像形成装置1000又は1000-2を画像形成装置1000として説明する。図33に示す第三のポリシー設定方法は、画像形成装置1000が最初にネットワーク5に接続した場合などのように、まだセキュリティポリシーを持っていない場合のポリシー設定方法である。

【0216】

図33において、画像形成装置1000に電源投入されると（ステップS31）、ネットワーク5を介して、ポリシー配布サーバ4000に対して、SOAPクライアント機能4023を利用して、ポリシー取得要求を行う（ステップS32）。ポリシー配布サーバ4000は、SOAPサーバ機能を利用して、ポリシー取得要求を受信し、ポリシー（管理者コンソール4001から受信したDSP2000）を受信結果として送信する。

【0217】

画像形成装置1000は、ポリシー配布サーバ4000からポリシーを受信すると、動作要件を満たすように動作する（ステップS33）。

【0218】

図34は、電源投入時にポリシーを取得する第四のポリシー設定方法を示す図である。

図34中、図33と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置1000又は1000-2を画像形成装置1000として説明する。図34において、ポリシー配布サーバ4000は、更に、識別情報比較部4029を有することである。

【0219】

画像形成装置1000に電源投入されると（ステップS41）、ネットワーク5を介して、ポリシー配布サーバ4000に対して、SOAPクライアント機能4023を利用して、ポリシー取得要求を行うと同時に、現在のDSP2000の識別情報（例えば、図23の記述211で示される「RDSP2023」）を同時に送信する（ステップS42）。

【0220】

ポリシー配布サーバ4000は、SOAPサーバ機能を利用して、ポリシー取得要求を受信すると、識別情報比較部4029によって、受信した識別情報（例えば、「RDSP2023」）と、配布するポリシーの識別情報とを比較する（ステップS43）。同じ場合は、同じ識別情報であるという受信結果だけを送信するようにする。同じでない場合に、ポリシー配布サーバ4000は画像形成装置1000に対して、受信結果としてポリシー（管理者コンソール4001から受信したDSP2000）を送信する（ステップS44）。

【0221】

画像形成装置1000は、ポリシー配布サーバ4000からポリシーを受信すると、受信したポリシーで保持していたポリシーを書き換えて、ポリシーに従って動作要件の選択を行い、動作要件を満たすように動作する（ステップS45）。

【0222】

この第二の変形例では、識別情報が同一である場合、ポリシーを配布しないため、無駄なトラフィックを軽減することができる。

【0223】

図35は、電源投入時にポリシーを取得する第五のポリシー設定方法を示す図である。図35中、図33と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置1000又は1000-2を画像形成装置1000として説明する。

【0224】

画像形成装置1000に電源投入されると（ステップS51）、ネットワーク5を介して、ポリシー配布サーバ4000に対して、SOAPクライアント機能4023を利用して、ポリシー配布要求を行う（ステップS52）。ポリシー配布サーバ4000は、SOAPサーバ機能4024によってポリシー配布要求を受信すると、受信結果を画像形成装置1000に送信する。

【0225】

その後、ポリシー配布サーバ4000は、SOAPクライアント機能4021によって、ポリシーを送信し、画像形成装置1000がそのポリシーを受信して、受信結果をポリシー配布サーバ4000へ返す（ステップS53）。

【0226】

画像形成装置1000は、ポリシー配布サーバ4000からポリシーを受信すると、ポリシーに従って動作要件の選択を行い、動作要件を満たすように動作する（ステップS54）。

【0227】

この第五のポリシー設定方法において、ポリシー配布サーバ4000は、画像形成装置1000からポリシー取得要求を受けた後速やかにポリシーを配布しても良いし、ポリシー取得要求を受けたことをポリシー配布サーバ4000の内部に記憶しておいて、所定のタイミングでポリシーを配布するようにしても良い。

【0228】

また、この第五のポリシー設定方法において、図34に示す第四のポリシー設定方法の

ように、ポリシー配布サーバ4000に識別情報比較部4029を備える構成としても良い。このような構成とすることによって、無駄なトラフィックを軽減することができる。

【0229】

図31から図36にて説明した第一及び第五のポリシー設定方法を実現するための機能構成について図36で説明する。図36は、第一から第五のポリシー設定方法を実現するための機能構成の例を示す図である。図36における説明において、画像形成装置1000と画像形成装置1000-2とは、同様の動作要件選択部1012を有するため、画像形成装置1000で説明する。また、点線の部分1002は、省略可能であることを示す。

【0230】

図36において、画像形成装置1000の動作要件選択部1012は、ポリシー解釈部4101と、選択要件検証部4102と、通信部4103と、ポリシー書き換え部4104と、DSP2000aと、システム属性91aとを有する。

【0231】

ポリシー解釈部4101は、ドキュメント属性取得部1011によって取得されたドキュメント属性と、ユーザ属性取得部1021によって取得されたユーザ属性とに対するポリシーを、DSP2000aに基づいて解釈する。そして、ポリシー解釈部4101は、その解釈結果として動作要件を選択要件検証部4102に通知する。つまり、ユーザが指定する動作を実行する際に満たさなければならない動作要件が通知される。

【0232】

選択要件検証部4102は、システム属性91aを参照することによって、ポリシー解釈部4101から通知された動作要件を満たすことができるか否かを判断する。そして、選択要件検証部4102は、その判断結果を動作制御部1013へ通知する。

【0233】

通信部4103は、SOAPに従ってポリシー配布サーバ4000との通信を制御する処理部であり、図31から図35に示すSOAPサーバ機能4022及びSOAPクライアント機能4023の少なくとも1つ以上を備えている。通信部4103は、ポリシー配布サーバ4000からポリシーとしてDSP2000bを受信すると、ポリシー書き換え部4104に通知する。また、図32に示すように、ポリシー配布サーバ4000に対して、ポリシー取得要求を行う際には、画像形成装置1000を認証するための認証情報を同時に送信する。

【0234】

ポリシー書き換え部4104は、受信したDSP2000bでDSP2000aを書き換える。また、ポリシー書き換え部4104は、図31に示されるように、認証情報がDSP2000bと同時に配布された場合、その認証情報に基づいてポリシー配布サーバ4000を認証し、ポリシー配布サーバ4000が認証された場合のみ、受信したDSP2000bでDSP2000aを書き換える。

【0235】

ポリシー配布サーバ4000は、通信部4123と、ポリシー管理部4124と、DSP2000bとを有する。

【0236】

通信部4123は、SOAPに従って画像形成装置1000との通信を制御する処理部であり、図31から図35に示すSOAPサーバ機能4021及びSOAPクライアント機能4024の少なくとも1つ以上を備えている。通信部4123は、DSP2000bを配布する。

【0237】

ポリシー管理部4124は、配布するDSP2000bを管理する。ポリシー管理部4124は、図31に示すように、通信部4123によって、DSP2000bを配布する際に、ポリシー配布サーバ4000を認証するための認証情報を同時に送信させる。また、ポリシー管理部4124は、ポリシー取得要求に画像形成装置1000の認証情報が同

時に送信された場合、その認証情報に基づいて画像形成装置 1 0 0 0 を認証し、認証できた場合のみ、ポリシーとして DSP 2 0 0 0 b を通信部 4 1 2 3 によって送信する。

【0238】

次に、タイマーによってポリシーを取得する第五のポリシー設定方法について図 3 7 で説明する。

【0239】

図 3 7 は、タイマーによってポリシーを取得する第六のポリシー設定方法を示す図である。図 3 7 中、図 3 3 と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置 1 0 0 0 又は 1 0 0 0 - 2 を画像形成装置 1 0 0 0 として説明する。

【0240】

図 3 7 において、画像形成装置 1 0 0 0 は、タイマー管理による処理時間が経過すると（ステップ S 5 1）、SOAP クライアント機能 4 0 2 3 を利用して、ポリシー配布サーバ 4 0 0 0 にポリシー取得要求を送信し、ポリシー配布サーバ 4 0 0 0 から SOAP サーバ機能 4 0 2 1 によって受信結果としてポリシー（管理コンソール 4 0 0 1 から受信した DSP 2 0 0 0）を送信する（ステップ S 5 2）。

【0241】

この第三のポリシー設定方法において、ポリシー配布サーバ 4 0 0 0 は SOAP クライアント機能 4 0 2 1 と SOAP サーバ機能 4 0 2 4 とを有するようにし、また、画像形成装置 1 0 0 0 は SOAP サーバ機能 2 2 と SOAP クライアント機能 4 0 2 3 とを有するようにして、画像形成装置 1 0 0 0 がポリシー取得要求を行った後にポリシーを配布するように構成しても良い。

【0242】

図 3 7 に示す第三のポリシー設定方法を実現する機能構成について図 3 8 で説明する。図 3 8 は、第六のポリシー設定方法を実現するための機能構成の例を示す図である。図 3 8 中、図 3 6 と同様の処理部には同一の符号を付し、その説明を省略する。また、画像形成装置 1 0 0 0 と画像形成装置 1 0 0 0 - 2 とは、同様の動作要件選択部 1 0 1 2 - 2 を有するため、画像形成装置 1 0 0 0 で説明する。また、点線の部分 1 0 0 2 は、省略可能であることを示す。

【0243】

図 3 6 に示す動作要件選択部 1 0 1 2 との違いは、動作要件選択部 1 0 1 2 - 2 が、タイマー部 4 1 0 5 を更に有することである。

【0244】

タイマー部 4 1 0 5 は、所定時間が経過すると、所定時間が経過したことを通信部 4 1 0 3 に通知する。この通知に応じて、通信部 4 1 0 3 は、ポリシー配布サーバ 4 0 0 0 から SOAP に従って DSP 2 0 0 0 b を取得し、ポリシー書き換え部 4 1 0 4 が DSP 2 0 0 0 a を DSP 2 0 0 0 b で書き換える。

【0245】

次に、オフラインでポリシーを設定する方法について図 3 9 で説明する。図 3 9 は、オフラインでポリシーを設定する第七のポリシー設定方法を示す図である。図 3 9 中、図 3 1 と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置 1 0 0 0 又は 1 0 0 0 - 2 を画像形成装置 1 0 0 0 として説明する。

【0246】

図 3 9 において、例えば、図 2 6 に示すようなハードディスク 5 1、光磁気ディスク 5 2、フレキシブルディスク 5 3、又は、光ディスク 5 4 の記憶媒体 5 0 に DSP 2 0 0 0 を格納し、その記憶媒体 5 0 を画像形成装置 1 0 0 0 に設定して DSP 2 0 0 0 を画像形成装置 1 0 0 0 の所定記憶領域に格納することによって、オフラインでポリシーを設定する（ステップ S 7 1）。

【0247】

その後、画像形成装置 1 0 0 0 は、所定格納領域にポリシーとして格納された DSP 2 0 0 0 に従って動作する（ステップ S 7 2）。

【 0 2 4 8 】

図 3 9 に示す第四のポリシー設定方法を実現する機能構成について説明する。図 4 0 は、第七のポリシー設定方法を実現するための機能構成の例を示す図である。図 4 0 中、図 3 6 と同様の処理部には同一の符号を付し、その説明を省略する。図 4 0 における説明において、画像形成装置 1 0 0 0 と画像形成装置 1 0 0 0 - 2 とは、同様の動作要件選択部 1 0 1 2 - 3 を有するため、画像形成装置 1 0 0 0 で説明する。また、点線の部分 1 0 0 2 は、省略可能であることを示す。

【 0 2 4 9 】

動作要件選択部 1 0 1 2 - 3 は、記憶媒体 5 0 から記憶媒体 5 0 に格納されている D S P 2 0 0 0 を読み取るためのインターフェース 4 1 0 6 を有するが、通信部 4 1 0 3 を含めない。

【 0 2 5 0 】

ポリシー書き換え部 4 1 0 4 は、インターフェース 4 1 0 6 によって読み込まれた D S P 2 0 0 0 を、動作要件選択部 1 0 1 2 0 3 が現在保持している D S P 2 0 0 0 a と書き換える。このようにして、オフラインの場合に、ポリシーが設定される。また、例えば、D S P 2 0 0 0 が格納された記憶媒体 5 0 によってオフラインでポリシーを設定する場合には、改ざん検知コードなどを追加することによって、ポリシーの信頼性を向上させることができる。

【 0 2 5 1 】

次に、ポリシーをオフラインで設定し、オンラインで選択する方法について図 4 1 で説明する。図 4 1 は、ポリシーをオフラインで設定し、オンラインで選択する第八のポリシー設定方法を示す。図 4 1 中、図 3 1 と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置 1 0 0 0 又は 1 0 0 0 - 2 を画像形成装置 1 0 0 0 として説明する。

【 0 2 5 2 】

図 4 1 において、管理者コンソール 4 0 0 1 からポリシー配布サーバ 4 0 0 0 へネットワーク 5 を介して、例えば、ポリシーとして D S P 2 0 0 0 が設定される（ステップ S 8 1）。

【 0 2 5 3 】

また、オフラインで D S P 2 0 0 0 が格納された記憶媒体 5 0（図 2 6 に示すようなハードディスク 5 1、光磁気ディスク 5 2、フレキシブルディスク 5 3、又は、光ディスク 5 4）が、画像形成装置 1 0 0 0 のセキュリティポリシーのデータベースに設定される（ステップ S 8 2）。

【 0 2 5 4 】

その後、管理コンソール 4 0 0 1 から、ネットワーク 5 を介して、ポリシー配布サーバ 4 0 0 0 にポリシーの選択が指定される（ステップ S 8 3）。ここで、ポリシーの選択とは、ポリシーの識別情報によってポリシーの 1 つが選択される。

【 0 2 5 5 】

ポリシー配布サーバ 4 0 0 0 は、管理コンソール 4 0 0 1 からのポリシー選択に応じて、S O A P クライアント機能 4 0 2 1 を利用して、画像形成装置 1 0 0 0 へポリシー選択を通知する（ステップ S 8 4）。画像形成装置 1 0 0 0 は、S O A P サーバ機能 4 0 2 2 を利用して、ポリシー選択通知を受信し、ポリシー配布サーバ 4 0 0 0 に対して受信結果を返す。つまり、執行すべきポリシーの識別情報が画像形成装置 1 0 0 0 に通知される。

【 0 2 5 6 】

画像形成装置 1 0 0 0 は、ポリシー選択に従って、識別情報で指定されるポリシーを選択し、その選択したポリシーに従って動作する（ステップ S 8 5）。

【 0 2 5 7 】

このような第五のポリシー設定方法を実現する機能構成について図 4 2 で説明する。図 4 2 は、第八のポリシー設定方法を実現するための機能構成の例を示す図である。図 4 2 中、図 3 6 及び図 4 0 と同様の処理部には同一の符号を付し、その説明を省略する。図 4

2における説明において、画像形成装置1000と画像形成装置1000-2とは、同様の動作要件選択部1012-4を有するため、画像形成装置1000で説明する。また、点線の部分1002は、省略可能であることを示す。

【0258】

動作要件選択部1012-4は、通信部4103を有すると共に、記憶媒体50から記憶媒体50に格納されているDSP2000を読み取るための記憶媒体50に対応したインターフェース4106を有する。

【0259】

通信部4103は、SOAPに従ってポリシー配布サーバ4000-2から受信したポリシー選択をポリシー書き換え部4012-2に通知する。

【0260】

ポリシー書き換え部4012-2は、例えば、オフラインのポリシー設定によって、インターフェース4106によって記憶媒体50に格納されたDSP2000を読み込んで、ドキュメントセキュリティポリシーDB92に格納する。ポリシー書き換え部4012-2は、通信部4103から通知されたポリシー選択に基づいて、執行すべきポリシーで置き換える。つまり、以前の執行すべきポリシーがDSP2000aであって、識別情報によってDSP2000が指定された場合、執行すべきポリシーとしてDSP2000aをDSP2000で書き換える。

【0261】

また、ポリシー配布サーバ4000-2が、DSP2000bを記憶媒体50に書き込むためのインターフェース4126を有する構成とすることによって、オフラインでポリシーを設定するために、ポリシー管理部4124がポリシー配布サーバ4000-2のDSP2000bを配布するポリシー（DSP2000）として記憶媒体50に書き込むようにしても良い。この場合の記憶媒体50は、図26に示すようなハードディスク51、光磁気ディスク52、フレキシブルディスク53、又は、光ディスク54等である。

【0262】

ポリシー配布サーバ4000-2において、通信部4123は、SOAPに従って、ポリシー選択を画像形成装置1000へ送信する。

【0263】

次に、ドキュメント属性とユーザ属性とに基づくポリシーの解釈を外部サーバに問い合わせる機能構成について図43及び44で説明する。

【0264】

図43は、外部サーバがポリシーを解釈する機能構成の例を示す図である。図43中、図36と同様の処理部には同一の符号を付し、その説明を省略する。図43における説明において、画像形成装置1000と画像形成装置1000-2とは、同様の動作要件選択部1012-3を有するため、画像形成装置1000で説明する。また、点線の部分1002は、省略可能であることを示す。

【0265】

画像形成装置1000側において、動作要件選択部1012-5は、通信部4103-2と、選択要件件勝負4102と、システム属性91aのみを有する。

【0266】

通信部4103-2は、ポリシー解釈サーバ4200とSOAPに従って通信を制御する処理部である。通信部4103-2は、ドキュメント属性取得部1011から通知されたドキュメント属性と、ユーザ属性取得部1021から通知されたユーザ属性とを、SOAPに従ってポリシー解釈サーバ4200に送信する。また、通信部4103-2は、ポリシー解釈サーバ4200からドキュメント属性とユーザ属性とに応じたルールを受信すると、選択要件検査部4102に通知する。ルールには、動作に対して許可する場合、満たさなければならない動作要件が示される。

【0267】

選択要件検証部4102は、システム属性91aを参照しつつ、動作要件を満たすこと

ができるか否かを判断し、その判断結果を動作制御部 1013 に通知する。

【0268】

外部サーバとしてのポリシー解釈サーバ 4200 は、サーバコンピュータであって、通信部 4213 と、ポリシー解釈部 4224 と、DSP 2000b とを有する。

【0269】

通信部 4213 は、SOAP に従って、画像形成装置 1000 との通信を制御する処理部であって、画像形成装置 1000 から受信したドキュメント属性とユーザ属性とをポリシー解釈部 4224 に通知し、ポリシー解釈部 4224 から通知されたドキュメント属性とユーザ属性とに対応するルールを画像形成装置 1000 へ送信する。ルールには動作が許可される場合の動作要件が含まれる。

【0270】

ポリシー解釈部 4224 は、通信部 4213 から取得したドキュメント属性とユーザ属性とに基づいて、DSP 2000b を参照することによって、動作が許可される場合の動作要件を含むルールを取得する。そのルールを通信部 4213 へ通知する。

【0271】

このような機能構成によって、画像形成装置 1000 がポリシーを保持していなくても、画像形成装置 1000 での動作に対してセキュリティポリシーを執行することができる。

【0272】

次に、外部サーバが、ポリシーを解釈し、更に選択要件を検証する機能構成について図 44 で説明する。

【0273】

図 44 は、外部サーバがポリシーを解釈し、選択要件を検証する機能構成の例を示す図である。図 44 中、図 43 と同様の処理部には同一の符号を付し、その説明を省略する。図 43 における説明において、画像形成装置 1000 と画像形成装置 1000-2 とは、同様の動作要件選択部 1012-3 を有するため、画像形成装置 1000 で説明する。また、点線の部分 1002 は、省略可能であることを示す。

【0274】

画像形成装置 1000 側において、動作要件選択部 1012-6 は、通信部 4103-3 のみを有する。

【0275】

通信部 4103-3 は、ポリシー解釈サーバ 4200 と SOAP に従って通信を制御する処理部である。通信部 4103-3 は、ドキュメント属性取得部 1011 から通知されたドキュメント属性と、ユーザ属性取得部 1021 から通知されたユーザ属性とを、SOAP に従ってポリシー解釈サーバ 4200-2 に送信する。また、通信部 4103-2 は、ポリシー解釈サーバ 4200 から動作に対する許可又は不許可と、許可する場合には動作要件とを受信し、動作制御部 1013 へ通知する。

【0276】

外部サーバとしての動作要件選択サーバ 4200-2 は、図 43 に示される構成に加えて、更に、選択要件検査部 4226 と、システム属性 91b とを有する。

【0277】

ポリシー解釈部 4224 は、通信部 4213 から取得したドキュメント属性とユーザ属性とに基づいて、DSP 2000b を参照することによって、動作が許可される場合の動作要件を含むルールを取得して、選択要件検証部 4226 へ通知する。

【0278】

選択要件検証部 4226 は、システム属性 91b を参照することによって、画像形成装置 1000 が動作要件を満たすことができるか否かを判断し、その判断結果を通信部 4213 によって画像形成装置 1000 へ送信する。動作要件を画像形成装置 1000 が満たすことができないと判断した場合、判断結果は不許可を示す。一方、動作要件を画像形成装置 1000 が満たすと判断した場合、判断結果は許可を示すと共に、動作要件を指定す

る。

【0279】

次に、画像形成装置1000の選択要件検証部4102によって参照される、画像形成装置1000内に備えられたシステム属性91aについて図45で説明する。図45は、画像形成装置内に備えられてシステム属性の例を示す図である。

【0280】

図45において、システム属性91aは、通常、ユーザの選択によって実行可能な動作条件の項目を管理するテーブルであって、動作条件、サポートの可否を示すサポート等の項目を有する。動作条件として、ログの記録、イメージログの記録、機密ラベルの印字、操作者ラベルの印字、識別バーコードの印字、識別パターンの印字等が示される。

【0281】

通常、動作条件は、動作する際の選択可能な機能として画像形成装置1000に備えられている。このような動作条件が、ポリシーによって動作を許可する場合の要件として指定される場合、動作要件となる。

【0282】

図46は、外部サーバに備えられたシステム属性の例を示す図である。図46において、システム属性91bは、動作条件毎に、複数の画像形成装置におけるサポート可否を、画像形成装置の識別情報（装置01、装置02、装置03、装置04、...）と対応付けて管理するテーブルである。動作条件として、ログの記録、イメージログの記録、機密ラベルの印字、操作者ラベルの印字、識別バーコードの印字、識別パターンの印字等が示される。

【0283】

通常、動作条件は、動作する際の選択可能な機能である。このような動作条件が、ポリシーによって動作を許可する場合の要件として指定される場合、動作要件となる。

【0284】

次に、画像形成装置1000又は1000-2とポリシー配布サーバ4000とで行われるポリシーを設定するためのSOAPの例について図47から図56で説明する。図47から図56の説明において、読み取り装置としての画像形成装置1000と複写装置としての画像形成装置1000-2とに何ら差異はないため、画像形成装置1000で説明する。

【0285】

先ず、図31に示されるように、ポリシー配布サーバ4000が、SOAPクライアント機能4021を利用して、画像形成装置1000にポリシー配布を行う場合のSOAPについて図47で説明する。図47は、SOAPに従って送信されるポリシー配布を示すXMLデータの例を示す図である。

【0286】

図47において、XMLデータ800は、ポリシーを配布するためのSOAPに従ったXMLによる記述である。XMLデータ800において、<ns1:policyDistribution>を示す記述801から</ns1:policyDistribution>を示す記述802までに、配布されるポリシーに関する情報と、ポリシー自身が示される。

【0287】

記述801において、「policyDistribution」により、このXMLデータ800がポリシーを配布することを示している。

【0288】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述803は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。そして、<policy xsi:type="xsd:string">から</policy>の記述804でポリシーが記述される。例えば、識別情報「RDSP2023」で識別されるDSP2000（図14から図22参照）そのものが記述される。

【0289】

そして、このようなポリシー配布を示すXMLデータ800を受信した画像形成装置1000は、SOAPサーバ機能4022を利用して、図48に示されるような受信結果をポリシー配布サーバ4000へ送信する。図48は、SOAPに従って送信されるポリシー配布に対する受信結果を示すXMLデータの例を示す図である。

【0290】

図48において、XMLデータ810は、ポリシー配布に対する受信結果を示すXMLによる記述である。XMLデータ810において、<ns1:policyDistributionResponse>を示す記述811から</ns1:policyDistributionResponse>を示す記述812までに、ポリシー配布に対する受信結果に関する情報が示される。

【0291】

記述812において、「policyDistributionResponse」によりこのXMLデータ810がポリシー配布に対する応答であることを示している。

【0292】

<result xsi:type="xsd:boolean">true</result>を示す記述813は、ポリシー配布を正常に受信したか否かを示す。この場合、「true」が示されるため、正常に受信したことを示している。

【0293】

図32に示されるように、ポリシー配布サーバ4000が、SOAPクライアント機能4021を利用して、画像形成装置1000にポリシー配布通知を行う場合のSOAPについて図49で説明する。図49は、SOAPに従って送信されるポリシー配布通知を示すXMLデータの例を示す図である。

【0294】

図49において、XMLデータ820は、ポリシー配布を通知するためのSOAPに従ったXMLによる記述である。XMLデータ820において、<ns1:policyDistributionReport>を示す記述821から</ns1:policyDistributionReport>を示す記述822までに、ポリシー配布通知に関する情報が示される。

【0295】

記述821において、「policyDistributionReport」により、このXMLデータ820がポリシー配布を通知することを示している。

【0296】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述823は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。

【0297】

そして、このようなポリシー配布通知を示すXMLデータ820を受信した画像形成装置1000は、SOAPサーバ機能4022を利用して受信結果を送信した後、SOAPクライアント機能4023を利用して、図50に示されるようなポリシー取得要求をポリシー配布サーバ4000へ送信する。図50は、SOAPに従って送信されるポリシー取得要求を示すXMLデータの例を示す図である。

【0298】

図50において、XMLデータ830は、ポリシーを配布するためのSOAPに従ったXMLによる記述である。XMLデータ830において、<ns1:policyRequest>を示す記述831から</ns1:policyRequest>を示す記述832までに、ポリシー取得要求に関する情報が示される。

【0299】

記述831において、「policyRequest」により、このXMLデータ830がポリシーの取得を要求していることを示している。

【0300】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述833は、図49に示されるポリシー配布通知を示すXMLデータ820で通知されたポリシーを識別するための識別情報「RDSP2023」が設定されている。

【0301】

このポリシー取得要求を示すXMLデータ830は、ポリシー配布通知を受信後、又は、処理のタイミングでポリシー配布サーバ4000に送信される。

【0302】

そして、このようなポリシー取得要求を示すXMLデータ830を受信したポリシー配布サーバ4000は、SOAPサーバ機能4024を利用して、図51に示されるような受信結果を画像形成装置1000へ送信する。図51は、SOAPに従って送信されるポリシー取得要に求対する受信結果を示すXMLデータの例を示す図である。

【0303】

図51において、XMLデータ840は、ポリシー取得要求に対する受信結果を示すXMLによる記述である。XMLデータ840において、<ns1:policyDistribution>を示す記述841から</ns1:policyDistribution>を示す記述842までに、配布されるポリシーに関する情報と、ポリシー自身が示される。

【0304】

記述841において、「policyDistribution」により、このXMLデータ840がポリシーを配布することを示している。

【0305】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述843は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。そして、<policy xsi:type="xsd:string">から</policy>の記述844でポリシーが記述される。例えば、識別情報「RDSP2023」で識別されるDSP2000（図14から図22参照）そのものが記述される。

【0306】

図52に示されるように、画像形成装置1000が、SOAPクライアント機能4023を利用して、ポリシー配布サーバ4000にポリシー配布要求を行う場合のSOAPについて図52で説明する。図52は、SOAPに従って送信されるポリシー配布要求を示すXMLデータの例を示す図である。

【0307】

図52において、XMLデータ850は、ポリシー配布を要求するためのSOAPに従ったXMLによる記述である。XMLデータ850において、<ns1:policyDistributionRequest>を示す記述851から</ns1:policyDistributionRequest>を示す記述852までに、ポリシー配布要求に関する情報が示される。

【0308】

記述851において、「policyDistributionRequest」により、このXMLデータ850がポリシー配布を通知することを示している。

【0309】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述853は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。

【0310】

そして、このようなポリシー配布要求を示すXMLデータ850を受信したポリシー配布サーバ4000は、受信後直に、或いは、所定のタイミングで図47に示すXMLデータ800によってポリシー配布を行う。

【0311】

図41に示されるように、ポリシー配布サーバ4000が、SOAPクライアント機能4021を利用して、画像形成装置1000へポリシー選択通知を行う場合のSOAPについて図53で説明する。図53は、SOAPに従って送信されるポリシー選択通知を示すXMLデータの例を示す図である。

【0312】

図53において、XMLデータ860は、ポリシー選択を通知するためのSOAPに従ったXMLによる記述である。XMLデータ860において、<ns1:policyChangeRequest

>を示す記述 8 6 1 から</ns1:policyChangeRequest>を示す記述 8 6 2 までに、選択すべきポリシーに関する情報が示される。

【0 3 1 3】

記述 8 6 1 において、「policyChangeRequest」により、このXMLデータ 8 6 0 がポリシー選択の通知であることを示している。

【0 3 1 4】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述 8 6 3 は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。画像形成装置 1 0 0 0 は、識別情報「RDSP2023」で識別されるポリシーを執行用のポリシーとして設定する。

【0 3 1 5】

次に、図 4 3 又は図 4 4 において、画像形成装置 1 0 0 0 がポリシーの解釈を行う外部サーバに動作要件取得要求を行う場合のSOAPについて図 5 4 及び図 5 5 で説明する。図 5 4 及び図 5 5 は、SOAPに従って送信される動作要件取得要求を示すXMLデータの例を示す図である。図 5 4 及び図 5 5 によって、一つのXMLデータ 8 7 0 が示される。

【0 3 1 6】

XMLデータ 8 7 0 において、図 5 4 の<ns1:isAllowed>を示す記述 8 7 1 から図 5 5 の</ns1:isAllowed>を示す記述 8 7 2 までに、ユーザ属性、ドキュメント属性、動作情報とが示される。

【0 3 1 7】

<userTicketInfo>を示す記述 8 7 3 から</userTicketInfo>を示す記述 8 7 4 によって、ユーザ属性が必要な場合のユーザチケットが指定される。例えば、図 4 3 において、外部サーバとしてのポリシー解釈サーバ 4 2 0 0 が、ポリシーを解釈するために、ユーザ属性が必要であると判断した場合、指定されるユーザチケットを用いてユーザ属性を取得する。

【0 3 1 8】

<docInfo xsi:type="ns1:DocInfo">から</docInfo>で示される記述 8 8 1 は、ドキュメント属性に関する情報を示す。記述 8 8 1 において、<catgory xsi:type="xsd:string">Technical_doc</category>を示す記述 8 8 2 は、ドキュメントのカテゴリーが「Technical_doc（技術関連文書）」であることを示し、<level xsi:type="xsd:string">High</level>を示す記述 8 8 3 は、ドキュメントのレベルが「High（高レベル）」であることを示し、<zone xsi:type="xsd:string">99.99.99.99</zone>を示す記述 8 8 4 は、ゾーンが「99.99.99.99」であることを示している。

【0 3 1 9】

また、<accessInfo>から</accessInfo>を示す記述 8 8 5 は、動作情報を示す。記述 8 8 5 において、<operation xsi:type="xsd:string">COPY</operation>を示す記述 8 8 6 は、動作がコピーであることを示している。

【0 3 2 0】

図 4 3 に示す外部サーバとしてのポリシー解釈サーバ 4 2 0 0 は、このようなXMLデータ 8 7 0 を受信すると、図 5 6 に示すようなポリシー解釈部 4 2 2 4 によるポリシー解釈結果を画像形成装置 1 0 0 0 へ送信する。図 5 6 は、SOAPに従って送信されるポリシー解釈結果を示すXMLデータの例を示す図である。

【0 3 2 1】

図 5 6 において、XMLデータ 8 9 0 は、ポリシー解釈結果を通知するためのSOAPに従ったXMLによる記述である。XMLデータ 8 9 0 において、<ns1:isAllowedResponse>を示す記述 8 9 1 から</ns1:isAllowedResponse>を示す記述 8 9 2 までに、ポリシー解釈結果に関する情報が示される。

【0 3 2 2】

記述 8 9 1 において、「isAllowedResponse」により、このXMLデータ 8 9 0 がポリシー解釈結果の通知を示している。

【 0 3 2 3 】

<allowed xsi:type="xsd:boolean">true</allowed>を示す記述 8 9 5 は、動作が許可されたことを示す。

【 0 3 2 4 】

また、<requirements>から</requirements>までの記述 8 9 6 は、動作を許可するための動作要件が示される。記述 8 9 6 において、<item>から</item>までの記述 8 9 7 は、動作要件を示す。<requirement xsi:type="xsd:string">audit</requirement>を示す記述によって、動作要件として監査証跡の記録（「audit」）が指定される。

【 0 3 2 5 】

次に、動作制御部 1 0 1 3 の機能構成について図 5 7 及び図 5 8 で説明する。先ず、図 2 8 に示す読み取り装置としての画像形成装置 1 0 0 0 の動作制御部 1 0 1 3 の機能構成について説明する。図 5 7 は、読み取り装置としての画像形成装置における動作制御部の機能構成の例を示す図である。

【 0 3 2 6 】

図 5 7 において、読み取り装置としての画像形成装置 1 0 0 0 において、動作制御部 1 0 1 3 は、データ処理部 7 4 を制御するデータ処理制御部 7 4 a と、データ送信部 7 5 を制御するデータ送信制御部 7 5 a とを有する。

【 0 3 2 7 】

読み取り装置としての画像形成装置 1 0 0 0 において、データ処理制御部 7 4 a は、例えば、動作要件選択部 1 0 1 2 から通知された動作要件に従って、読み取り処理を停止し、必要に応じて読み取ったデータを全て消去する、読み取ったデータの一部を黒くする、白くする、又はページを削除する等によって消去する、カラー情報を消去する、情報量を低減する、「丸秘」スタンプを印字することによって機密ラベルを追加する、また、バーコード、数字、文字、パターン、セキュリティ属性を印字することによって識別情報を追加する、などを実行するようにデータ処理部 7 4 を制御する。

【 0 3 2 8 】

読み取り装置としての画像形成装置 1 0 0 0 において、データ送信制御部 7 5 a は、例えば、動作要件選択部 1 0 1 2 から通知された動作要件に従って、送信を停止する、動作要件で指定された送信先だけに送信する、動作要件で指定された送信先にも送信する、などを実行するようにデータ送信部 7 5 を制御する。

【 0 3 2 9 】

図 5 8 は、複写装置としての画像形成装置における動作制御部の機能構成の例を示す図である。

【 0 3 3 0 】

図 5 8 において、複写装置としての画像形成装置 1 0 0 0 - 2 において、動作制御部 1 0 1 3 は、データ処理部 7 4 を制御するデータ処理制御部 7 4 a と、印刷部 7 6 を制御する印刷制御部 7 6 a とを有する。

【 0 3 3 1 】

複写装置としての画像形成装置 1 0 0 0 - 2 において、データ処理制御部 7 4 a は、図 5 7 の読み取り装置としての画像形成装置 1 0 0 0 におけるデータ処理制御部 7 4 a と同様であって、例えば、動作要件選択部 1 0 1 2 から通知された動作要件に従って、読み取り処理を停止し、必要に応じて読み取ったデータを全て消去する、読み取ったデータの一部を黒くする、白くする、又はページを削除する等によって消去する、カラー情報を消去する、情報量を低減する、「丸秘」スタンプを印字することによって機密ラベルを追加する、また、バーコード、数字、文字、パターン、セキュリティ属性を印字することによって識別情報を追加する、などを実行するようにデータ処理部 7 4 を制御する。

【 0 3 3 2 】

複写装置としての画像形成装置 1 0 0 0 - 2 において、印刷制御部 7 6 a は、例えば、印刷を停止する、動作要件で指定されたトレイの用紙に印刷する、などを実行するように印刷制御部 7 6 a を制御する。

【0 3 3 3】

上記実施例において、読み取り装置としての画像形成装置 1 0 0 0 と、複写装置としての画像形成装置 1 0 0 0 - 2 について例示したが、プリンタ、F A X、コピー等の複数の異なる画像形成機能の少なくとも 1 つを有する装置又はこのような複数の異なる画像形成機能を有する装置であっても良い。

【0 3 3 4】

本発明によれば、ドキュメントに関する企業内のセキュリティポリシーを外部から設定できるため、企業内を一貫したセキュリティポリシーによってドキュメントの取り扱いを制御することができる。また、ドキュメントが紙原稿であっても電子データ（ドキュメントデータ）であっても、セキュリティポリシーに従った制御を実行することができる。

【図面の簡単な説明】

【0 3 3 5】

- 【図 1】セキュリティポリシーの例を示す図である。
- 【図 2】ドキュメントラベル用語ファイルのリストの例を示す図である。
- 【図 3】ポリシー用語ファイルの例を示す図である。
- 【図 4】ポリシー用語ファイルの例を示す図である。
- 【図 5】ポリシー用語ファイルの例を示す図である。
- 【図 6】ポリシー用語ファイルの例を示す図である。
- 【図 7】ポリシー用語ファイルの例を示す図である。
- 【図 8】ポリシー用語ファイルの例を示す図である。
- 【図 9】ポリシー用語ファイルの例を示す図である。
- 【図 1 0】ポリシー用語ファイルの例を示す図である。
- 【図 1 1】ポリシー用語ファイルの例を示す図である。
- 【図 1 2】ポリシー用語ファイルの例を示す図である。
- 【図 1 3】ポリシー用語ファイルの例を示す図である。
- 【図 1 4】ポリシーファイルの例を示す図である。
- 【図 1 5】ポリシーファイルの例を示す図である。
- 【図 1 6】ポリシーファイルの例を示す図である。
- 【図 1 7】ポリシーファイルの例を示す図である。
- 【図 1 8】ポリシーファイルの例を示す図である。
- 【図 1 9】ポリシーファイルの例を示す図である。
- 【図 2 0】ポリシーファイルの例を示す図である。
- 【図 2 1】ポリシーファイルの例を示す図である。
- 【図 2 2】ポリシーファイルの例を示す図である。
- 【図 2 3】D S P の識別情報の例を示す図である。
- 【図 2 4】D S P の構造を説明するための記述例を示す図である。
- 【図 2 5】D S P の他の記述例を示す図である。
- 【図 2 6】D S P を蓄積し且つ配布する種々の媒体を示す図である。
- 【図 2 7】本発明の一実施例に係る画像形成装置のハードウェア構成を示すブロック図である。
- 【図 2 8】セキュリティポリシーに従って動作する読み取り装置としての画像形成装置の機能構成を示す図である。
- 【図 2 9】簡略化した D S P の例を示す図である。
- 【図 3 0】セキュリティポリシーに従って動作する複写装置としての画像形成装置の機能構成を示す図である。
- 【図 3 1】外部サーバからポリシーが配布される第一のポリシー設定方法を示す図である。
- 【図 3 2】外部サーバからポリシーを取得する第二のポリシー設定方法を示す図である。
- 【図 3 3】電源投入時にポリシーを取得する第三のポリシー設定方法を示す図である。

- 。
- 【図 3 4】電源投入時にポリシーを取得する第四のポリシー設定方法を示す図である。
- 。
- 【図 3 5】電源投入時にポリシーを取得する第五のポリシー設定方法を示す図である。
- 。
- 【図 3 6】第一から第五のポリシー設定方法を実現するための機能構成の例を示す図である。
- 【図 3 7】タイマーによってポリシーを取得する第六のポリシー設定方法を示す図である。
- 【図 3 8】第六のポリシー設定方法を実現するための機能構成の例を示す図である。
- 【図 3 9】オフラインでポリシーを設定する第七のポリシー設定方法を示す図である。
- 。
- 【図 4 0】第七のポリシー設定方法を実現するための機能構成の例を示す図である。
- 【図 4 1】ポリシーをオフラインで設定し、オンラインで選択する第八のポリシー設定方法を示す。
- 【図 4 2】第八のポリシー設定方法を実現するための機能構成の例を示す図である。
- 【図 4 3】外部サーバがポリシーを解釈する機能構成の例を示す図である。
- 【図 4 4】外部サーバがポリシーを解釈し、選択要件を検証する機能構成の例を示す図である。
- 【図 4 5】画像形成装置内に備えられてシステム属性の例を示す図である。
- 【図 4 6】外部サーバに備えられたシステム属性の例を示す図である。
- 【図 4 7】S O A P に従って送信されるポリシー配布を示すXMLデータの例を示す図である。
- 【図 4 8】S O A P に従って送信されるポリシー配布に対する受信結果を示すXMLデータの例を示す図である。
- 【図 4 9】S O A P に従って送信されるポリシー配布通知を示すXMLデータの例を示す図である。
- 【図 5 0】S O A P に従って送信されるポリシー取得要求を示すXMLデータの例を示す図である。
- 【図 5 1】S O A P に従って送信されるポリシー取得要求に対する受信結果を示すXMLデータの例を示す図である。
- 【図 5 2】S O A P に従って送信されるポリシー配布要求を示すXMLデータの例を示す図である。
- 【図 5 3】S O A P に従って送信されるポリシー選択通知を示すXMLデータの例を示す図である。
- 【図 5 4】S O A P に従って送信されるポリシー選択通知を示すXMLデータの例を示す図である。
- 【図 5 5】S O A P に従って送信されるポリシー配布を示すXMLデータの例を示す図である。
- 【図 5 6】S O A P に従って送信されるポリシー解釈結果を示すXMLデータの例を示す図である。
- 【図 5 7】読み取り装置としての画像形成装置における動作制御部の機能構成の例を示す図である。
- 【図 5 8】複写装置としての画像形成装置における動作制御部の機能構成の例を示す図である。

【符号の説明】

【0 3 3 6】

- | | |
|-----|------------|
| 5 1 | ハードディスク |
| 5 2 | 光磁気ディスク |
| 5 3 | フレキシブルディスク |

5 4	光ディスク
5 5	コンピュータ
5 6	ネットワーク
7 1	読み取り部
7 2	読み取り条件取得部
7 3	データ送信先取得部
7 4	データ処理部
1 0 0 0	画像形成装置
1 0 0 1	ポリシー実行部
1 0 1 1	ドキュメント属性取得部
1 0 1 2	動作要件選択部
1 0 1 3	動作制御部
1 0 2 1	ユーザ属性取得部
2 0 0 0	D S P

【書類名】図面
【図 1】

ドキュメントに関するセキュリティポリシーの例を示す図

201
~

202 ~ 極秘文書について:

原則複写禁止 (複写する際には管理責任者の許可を得なければならない),
また, 複写したことを記録しておかなければならない
プリントする際には複写禁止であることを示す透かしを入れなければならない
ない, また, プリントしたことを記録しておかなければならない
閲覧は関係者のみ許可

203 ~ 丸秘文書について:

複写は関係者のみ許可

プリントする際には丸秘文書であることを示すラベルを同時に印刷しな
ければならない

閲覧は関係者のみ許可

204 ~ 社外秘文書について:

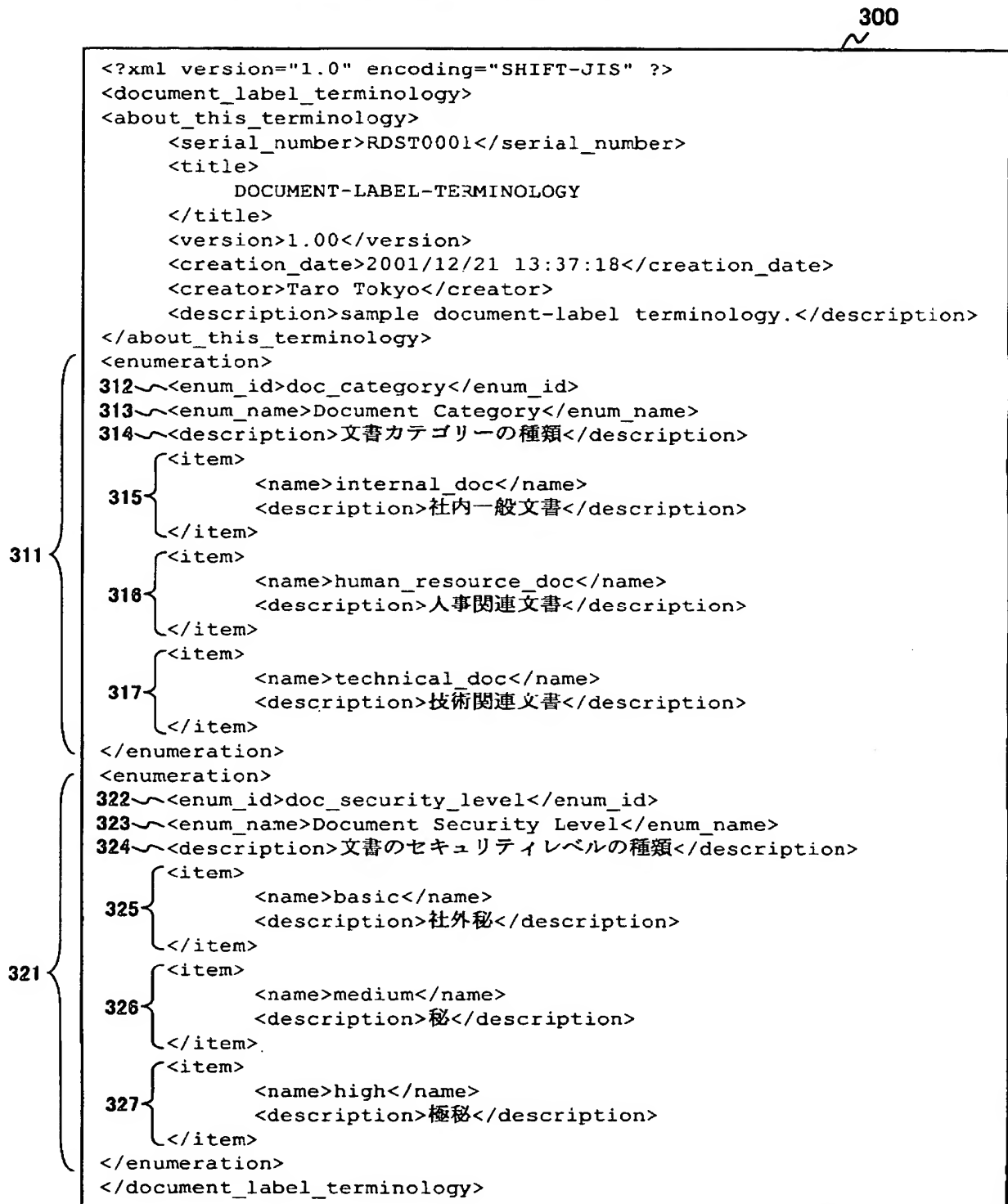
社外へ送付する際には管理責任者の許可を得なければならない
複写 プリント 閲覧は社内であれば許可不要

205 ~ 人事関連文書について:

すべて丸秘文書として取り扱う

【図 2】

ドキュメントラベルファイルの例を示す図



【図 3】

ポリシー用語ファイルの例を示す図

400

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<policy_terminology>
  <about_this_terminology>
    <serial_number>RDST9487</serial_number>
    <title>DOCUMENT-SECURITY-POLICY-TERMINOLOGY</title>
    <version>1.00</version>
    <creation_date>2001/12/21 13:37:18</creation_date>
    <creator>Taro Tokyo</creator>
    <description>sample policy terminology.</description>
  </about_this_terminology>

  <!-- システムタイプの列挙 -->
  <enumeration>
    <enum_id>system_type</enum_id>
    <enum_name>System Type</enum_name>
    <description>システムタイプの種類</description>
    <item>
      <name>Copier</name>
      <description>複写機</description>
      <operation>copier_operation</operation>
    </item>
    <item>
      <name>Printer</name>
      <description>プリンタ</description>
      <operation>printer_operation</operation>
    </item>
    <item>
      <name>Facsimile</name>
      <description>ファクシミリ</description>
      <operation>fax_operation</operation>
    </item>
    <item>
      <name>Scanner</name>
      <description>スキャナ</description>
      <operation>scanner_operation</operation>
    </item>
    <item>
      <name>Document Repository</name>
      <description>文書リポジトリ</description>
      <operation>repository_operation</operation>
    </item>
    <item>
      <name>E-Meeting</name>
      <description>電子会議システム</description>
      <operation>emeeting_operation</operation>
    </item>
  </enumeration>
```

411

【図 4】

ポリシー用語ファイルの例を示す図

```
400 ~
<!-- システムタイプごとのオペレーションの列挙 -->
<enumeration>
  <enum_id>copier_operation</enum_id>
  <enum_name>Copier Operation</enum_name>
  <description>複写機に関わるオペレーション</description>
  <item>
    <name>hardcopy</name>
    <description>紙から紙への複写</description>
    <requirement>hardcopy_requirement</requirement>
  </item>
</enumeration>
421 ~
<enumeration>
  <enum_id>printer_operation</enum_id>
  <enum_name>Printer Operation</enum_name>
  <description>プリンタに関わるオペレーション</description>
  <item>
    <name>print</name>
    <description>電子文書を紙へ印刷</description>
    <requirement>print_requirement</requirement>
  </item>
</enumeration>
431 ~
<enumeration>
  <enum_id>fax_operation</enum_id>
  <enum_name>Facsimile Operation</enum_name>
  <description>ファックスに関わるオペレーション</description>
  <item>
    <name>fax_send</name>
    <description>ファックスの送信</description>
    <requirement>fax_send_requirement</requirement>
  </item>
  <item>
    <name>fax_receive</name>
    <description>ファックスの受信</description>
    <requirement>fax_receive_requirement</requirement>
  </item>
</enumeration>
441 ~
<enumeration>
  <enum_id>scanner_operation</enum_id>
  <enum_name>Scanner Operation</enum_name>
  <description>スキャナに関わるオペレーション</description>
  <item>
    <name>scan</name>
    <description>紙文書をスキャンして電子文書にする</description>
    <requirement>scan_requirement</requirement>
  </item>
</enumeration>
451 ~
</enumeration>
```


【図5】

ポリシー用語ファイルの例を示す図

```
400 ~
<enumeration>
  <enum_id>repository_operation</enum_id>
  <enum_name>Document Repository Operation</enum_name>
  <description>文書リポジトリに関わるオペレーション</description>
  <item>
    <name>store</name>
    <description>保存する</description>
    <requirement>store_requirement</requirement>
  </item>
  <item>
    <name>revise</name>
    <description>改訂・編集する</description>
    <requirement>revise_requirement</requirement>
  </item>
  <item>
    <name>delete</name>
    <description>削除・破棄する</description>
    <requirement>delete_requirement</requirement>
  </item>
  <item>
    <name>read</name>
    <description>参照する</description>
    <requirement>read_requirement</requirement>
  </item>
  <item>
    <name>net_delivery</name>
    <description>
      ネットワークで配布する（送信する）
    </description>
    <requirement>net_delivery_requirement</requirement>
  </item>
  <item>
    <name>disc_delivery</name>
    <description>ディスクで配布する（送付する）</description>
    <requirement>disc_delivery_requirement</requirement>
  </item>
  <item>
    <name>archive</name>
    <description>アーカイブ・バックアップする</description>
    <requirement>archive_requirement</requirement>
  </item>
</enumeration>
461 ~
<enumeration>
  <enum_id>emeeting_operation</enum_id>
  <enum_name>E-Meeting Operation</enum_name>
  <description>電子会議システムに関わるオペレーション</description>
  <item>
    <name>meeting_use</name>
    <description>会議で利用する</description>
    <requirement>meeting_use_requirement</requirement>
  </item>
</enumeration>
471 ~
```

【図 6】

ポリシー用語ファイルの例を示す図

400

```
<!-- オペレーションごとに適用できる要件の列挙 -->
<!-- ユーザ認証, 文書識別, アクセス制御 (利用制限) は基本メカニズムとして提供されるため,
要件には含めない -->
```

481

```
<enumeration>
  <enum_id>hardcopy_requirement</enum_id>
  <enum_name>Hardcopy Requirement</enum_name>
  <description>複写に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
</enumeration>
```

491

```
<enumeration>
  <enum_id>print_requirement</enum_id>
  <enum_name>Print Requirement</enum_name>
  <description>印刷に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>private_access</name>
    <description>プリントした本人による紙出力</description>
  </item>
  <item>
    <name>trusted_channel</name>
    <description>
      信頼チャネルの利用 (印刷データの暗号化)
    </description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>
      プリントアウトに追跡情報埋め込み (透かし, ラベル, バーコード)
    </description>
  </item>
</enumeration>
```

【図7】

ポリシー用語ファイルの例を示す図

400 ~

```
<enumeration>
  <enum_id>fax_send_requirement</enum_id>
  <enum_name>Requirement on Sending Fax Message</enum_name>
  <description>ファクス送信に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>destination_restriction</name>
    <description>宛先制限</description>
  </item>
  <item>
    <name>private_mode</name>
    <description>親展モードでの送信</description>
  </item>
  <item>
    <name>trusted_channel</name>
    <description>
      信頼チャネルの利用（ファクスデータの暗号化）
    </description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>
      送信ファクスに追跡情報埋め込み（透かし、ラベル、バーコード）
    </description>
  </item>
  <item>
    <name>non_repudiation</name>
    <description>否認防止（受取証の取得）</description>
  </item>
</enumeration>
```

501 ~

【図 8】

ポリシー用語ファイルの例を示す図

```

400 ~
<enumeration>
  <enum_id>fax_receive_requirement</enum_id>
  <enum_name>Requirement on Receiving Fax Message</enum_name>
  <description>ファックス受信に関わる要件</description>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>private_access</name>
    <description>親展ファックスの宛先本人による取り出し</description>
  </item>
  <item>
    <name>trusted_timestamp</name>
    <description>信頼タイムスタンプ</description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>
      受信ファックスに追跡情報埋め込み (透かし, ラベル, バーコード)
    </description>
  </item>
</enumeration>
511 ~
<enumeration>
  <enum_id>scan_requirement</enum_id>
  <enum_name>Scan Requirement</enum_name>
  <description>スキャンに関わる要件 (保存した後については保存要件を適用する)
  </description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>
      スキャン画像に追跡情報埋め込み (透かし, ラベル, バーコード)
    </description>
  </item>
</enumeration>
521 ~

```

【図 9】

ポリシー用語ファイルの例を示す図

```

400 ~
<enumeration>
  <enum_id>store_requirement</enum_id>
  <enum_name>Store Requirement</enum_name>
  <description>保存に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>encryption</name>
    <description>保存データの暗号化</description>
  </item>
  <item>
    <name>integrity_protection</name>
    <description>保存データの改ざん保護</description>
  </item>
</enumeration>
531 ~
<enumeration>
  <enum_id>revise_requirement</enum_id>
  <enum_name>Revise Requirement</enum_name>
  <description>改訂に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>versioning</name>
    <description>バージョン管理</description>
  </item>
</enumeration>
541 ~

```

【図 10】

ポリシー用語ファイルの例を示す図

```
400 ~
<enumeration>
  <enum_id>delete_requirement</enum_id>
  <enum_name>Delete Requirement</enum_name>
  <description>削除・破棄に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>complete_erase</name>
    <description>完全消去</description>
  </item>
</enumeration>
551 ~
<enumeration>
  <enum_id>read_requirement</enum_id>
  <enum_name>Read Requirement</enum_name>
  <description>参照に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>edit_restriction</name>
    <description>編集禁止のデータのみ参照許可</description>
  </item>
  <item>
    <name>print_restriction</name>
    <description>印刷禁止のデータのみ参照許可</description>
  </item>
  <item>
    <name>location_restriction</name>
    <description>参照場所限定のデータのみ参照許可</description>
  </item>
  <item>
    <name>user_restriction</name>
    <description>ユーザ限定のデータのみ参照許可</description>
  </item>
</enumeration>
561 ~
```

【図 11】

ポリシー用語ファイルの例を示す図

400 ~

```
<enumeration>
  <enum_id>net_delivery_requirement</enum_id>
  <enum_name>Delivery via Network Requirement</enum_name>
  <description>ネットワーク配信（送信）に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>trusted_channel</name>
    <description>信頼チャネルの利用（送信データの暗号化）
  </description>
  </item>
  <item>
    <name>destination_restriction</name>
    <description>宛先制限（社内のみ配信可能など）</description>
  </item>
  <item>
    <name>edit_restriction</name>
    <description>編集禁止のデータのみ配信許可</description>
  </item>
  <item>
    <name>print_restriction</name>
    <description>印刷禁止のデータのみ配信許可</description>
  </item>
  <item>
    <name>location_restriction</name>
    <description>参照場所限定のデータのみ配信許可</description>
  </item>
  <item>
    <name>user_restriction</name>
    <description>ユーザ限定のデータのみ配信許可</description>
  </item>
</enumeration>
```

571 ~

【図 12】

ポリシー用語ファイルの例を示す図

400 ~

```
<enumeration>
  <enum_id>disc_delivery_requirement</enum_id>
  <enum_name>Delivery via Disc Requirement</enum_name>
  <description>ディスク配布（送付）に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>encryption</name>
    <description>送付データの暗号化</description>
  </item>
  <item>
    <name>integrity_protection</name>
    <description>送付データの改ざん保護</description>
  </item>
  <item>
    <name>edit_restriction</name>
    <description>編集禁止のデータのみ送付許可</description>
  </item>
  <item>
    <name>print_restriction</name>
    <description>印刷禁止のデータのみ送付許可</description>
  </item>
  <item>
    <name>location_restriction</name>
    <description>参照場所限定のデータのみ送付許可</description>
  </item>
  <item>
    <name>user_restriction</name>
    <description>ユーザ限定のデータのみ送付許可</description>
  </item>
</enumeration>
```

581 ~

【図 13】

ポリシー用語ファイルの例を示す図

```
400 ~
{
  <enumeration>
    <enum_id>archive_requirement</enum_id>
    <enum_name>Archive Requirement</enum_name>
    <description>アーカイブ・バックアップに関わる要件</description>
    <item>
      <name>explicit_authorization</name>
      <description>明示的な許可（利用制限）</description>
    </item>
    <item>
      <name>audit</name>
      <description>監査証跡の記録</description>
    </item>
    <item>
      <name>encryption</name>
      <description>アーカイブデータの暗号化</description>
    </item>
    <item>
      <name>integrity_protection</name>
      <description>アーカイブデータの改ざん保護</description>
    </item>
  </enumeration>
  <enumeration>
    <enum_id>meeting_use_requirement</enum_id>
    <enum_name>Meeting-use Requirement</enum_name>
    <description>会議での利用に関わる要件</description>
    <item>
      <name>explicit_authorization</name>
      <description>明示的な許可（利用制限）</description>
    </item>
    <item>
      <name>audit</name>
      <description>監査証跡の記録</description>
    </item>
    <item>
      <name>audit_with_image</name>
      <description>監査証跡のイメージ付き記録</description>
    </item>
  </enumeration>
</policy_terminology>
591 ~
601 ~
```

【図 14】

ポリシーファイルの例を示す図

```

2000 ~
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
  <about_this_policy>
    <serial_number>RDSP2023</serial_number>
    <terminology_applied>RDST9487</terminology_applied>
    <title>DOCUMENT-SECURITY-POLICY</title>
    <version>1.30</version>
    <creation_date>2002/02/18 22:30:24</creation_date>
    <creator>Taro Tokyo</creator>
    <description>sample document security policy.</description>
  </about_this_policy>
2001 ~ <policy>
  <acc_rule> ~ 2011
2013 { <doc_category>ANY</doc_category>
      <doc_security_level>basic</doc_security_level>
      <acl>
        <ace>
          2017 { <user_category>ANY</user_category>
                <user_security_level>ANY</user_security_level>
                <operation>
                  <name>hardcopy</name>
                  <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                  <name>print</name>
                  <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                  <name>fax_send</name>
                  <requirement>audit</requirement>
                  <requirement>explicit_authorization</requirement>
                </operation>
                <operation>
                  <name>fax_receive</name>
                  <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                  <name>scan</name>
                  <allowed/><!-- allowed without any requirement -->
                </operation>
              }
            }
  }
~

```

【図 15】

ポリシーファイルの例を示す図

2000

```
<operation>
  <name>store</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>revise</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>delete</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>read</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>net_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
  <requirement>trusted_channel</requirement>
</operation>
<operation>
  <name>disc_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>meeting_use</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
</ace>
</acl>
</acc_rule> ~ 2012
```

【図 16】

ポリシーファイルの例を示す図

2000

```

<acc_rule>~2021
2023 { <doc_category>ANY</doc_category>
      <doc_security_level>medium</doc_security_level>
      <acl>
        <ace>
          2027 { <user_category>DOC-CATEGORY</user_category>
                <user_security_level>ANY</user_security_level>
                <operation>
                  <name>hardcopy</name>
                  <requirement>audit</requirement>
                  <requirement>embed_trace_info</requirement>
                </operation>
                <operation>
                  <name>print</name>
                  <requirement>audit</requirement>
                  <requirement>embed_trace_info</requirement>
                </operation>
                <operation>
                  <name>fax_send</name>
                  <denied/>
                  <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                  <name>fax_receive</name>
                  <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                  <name>scan</name>
                  <requirement>audit</requirement>
                  <requirement>embed_trace_info</requirement>
                </operation>
                <operation>
                  <name>store</name>
                  <allowed/><!-- allowed without any requirement -->
                </operation>
              }
        }
      }
    }
  
```

【図 17】

ポリシーファイルの例を示す図

2000

```
<operation>
  <name>revise</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>delete</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>read</name>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
  <requirement>trusted_channel</requirement>
</operation>
<operation>
  <name>disc_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>meeting_use</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
</ace>
```

【図 18】

ポリシーファイルの例を示す図

2000

```
<acc>
2028 { <user_category>ANY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>hardcopy</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>print</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_send</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_receive</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>scan</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>store</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>revise</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>delete</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
    }
```

【図 19】

ポリシーファイルの例を示す図

2000

```

<operation>
  <name>read</name>
  <requirement>explicit_authorization</requirement>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>disc_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>archive</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>meeting_use</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
</ace>
</acl>
</acc_rule> ~ 2022
<acc_rule> ~ 2031
2033 { <doc_category>ANY</doc_category>
      <doc_security_level>high</doc_security_level>
      <acl>
        <ace>
          2037 { <user_category>DOC-CATEGORY</user_category>
                <user_security_level>ANY</user_security_level>
                <operation>
                  <name>hardcopy</name>
                  <denied/>
                  <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                  <name>print</name>
                  <requirement>explicit_authorization</requirement>
                  <requirement>audit</requirement>
                  <requirement>private_access</requirement>
                  <requirement>trusted_channel</requirement>
                  <requirement>embed_trace_info</requirement>
                </operation>

```

【図 20】

ポリシーファイルの例を示す図

2000

```
<operation>
  <name>fax_send</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>fax_receive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>scan</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>store</name>
  <requirement>audit</requirement>
  <requirement>encryption</requirement>
  <requirement>integrity_protection</requirement>
</operation>
<operation>
  <name>revise</name>
  <requirement>versioning</requirement>
</operation>
<operation>
  <name>delete</name>
  <requirement>complete_erase</requirement>
</operation>
<operation>
  <name>read</name>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
  <requirement>user_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
```


【図 21】

ポリシーファイルの例を示す図

2000

```
<operation>
  <name>disc_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>encryption</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <requirement>encryption</requirement>
  <requirement>integrity_protection</requirement>
</operation>
<operation>
  <name>meeting_use</name>
  <requirement>explicit_authorization</requirement>
</operation>
</ace>
<ace>
2038 { <user_category>ANY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>hardcopy</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>print</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_send</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_receive</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>scan</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
    }
  </ace>
```

【図 22】

ポリシーファイルの例を示す図

2000

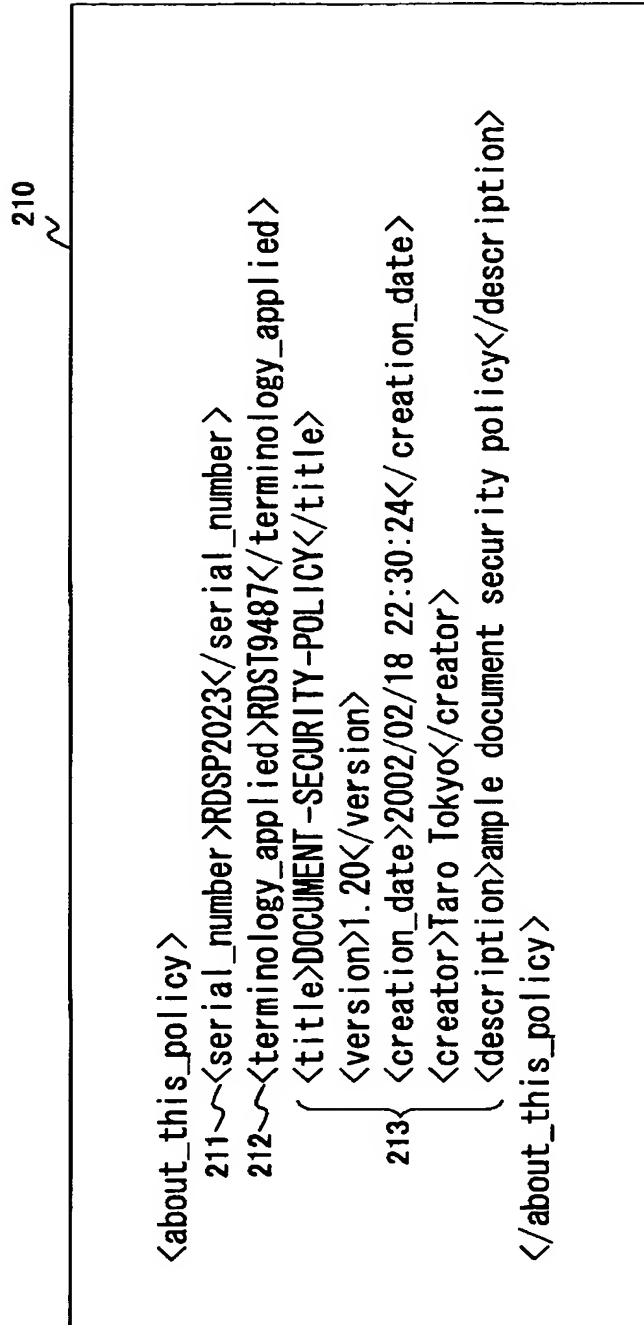
```

<operation>
  <name>store</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>revise</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>delete</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>read</name>
  <requirement>explicit_authorization</requirement>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
  <requirement>user_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>disc_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>archive</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>meeting_use</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
</ace>
</acl>
</acc_rule>
2002
</policy>
</document_security_policy>

```

【図 23】

DSPの識別情報を示す図



【図 24】

DSPの構造を説明するための記述例を示す図

220

```

<policy>
221 ~<acc_rule>
    232 { <doc_category>ANY</doc_category>
        <doc_security_level>medium</doc_security_level>
    223 ~<acl>
        224 ~<ace>
            225 ~<user_category>DOC-CATEGORY
                </user_category>
            226 ~<user_security_level>ANY
                </user_security_level>
            227 ~<operation>
                228 ~<name>fax_send</name>
                229 ~<denied/><!-- denied even if it
                    is explicitly authorized -->
                </operation>
            227 ~<operation>
                <name>net_delivery</name>
                230 ~<requirement>audit
                    </requirement>
                231 ~<requirement>
                    explicit_authorization
                </requirement>
                ...
            </operation>
            227 ~<operation>
                <name>fax_receive</name>
                232 ~<allowed/><!--allowed
                    without requirements -->
                </operation>
                ...
            </ace>
            <ace>
                ...
            </ace>
        </acl>
    </acc_rule>
221 ~<acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
        ...
    </acl>
    </acc_rule>
</policy>

```

【図 25】

DSPの他の記述例を示す図

240

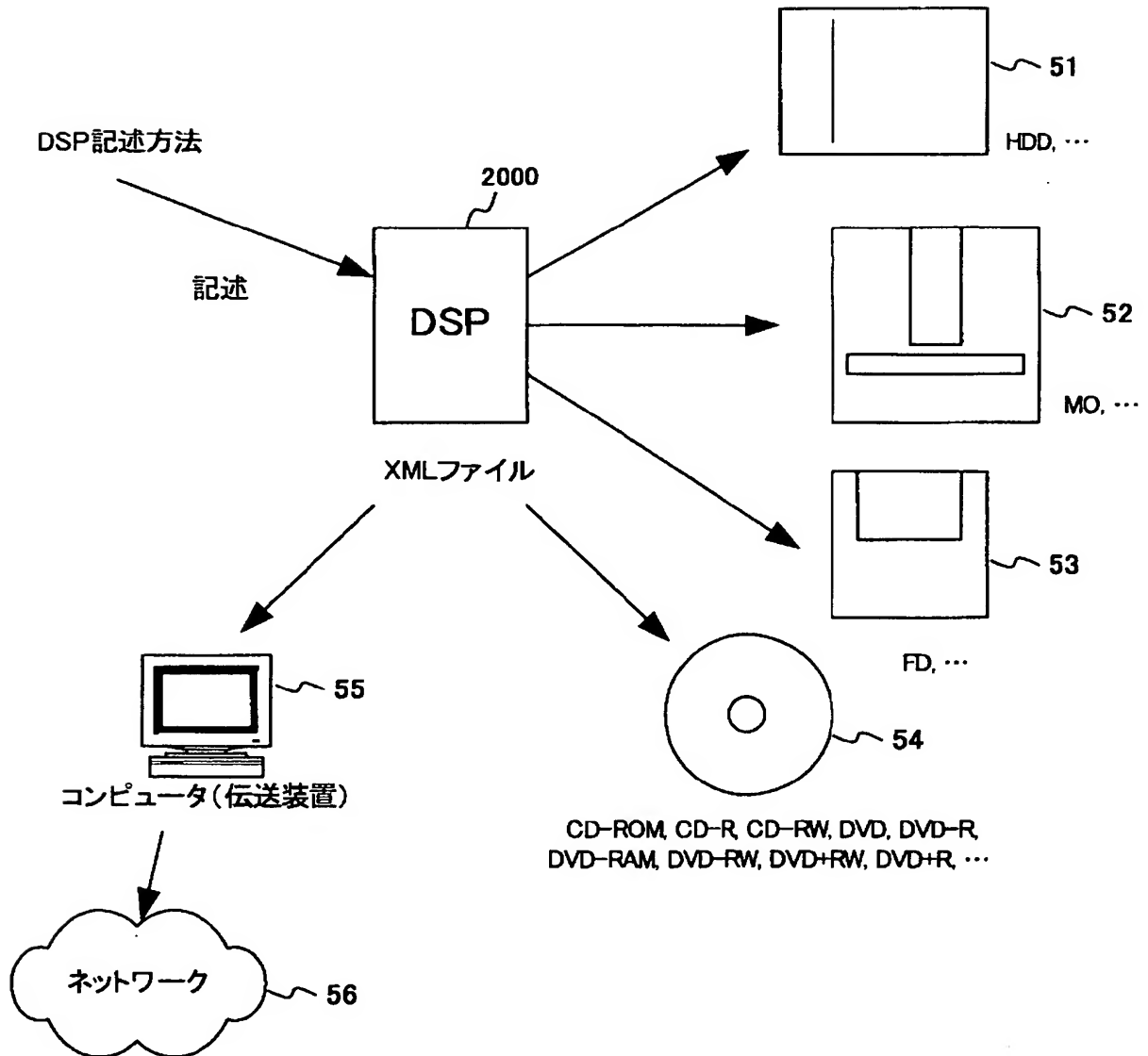
```

<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>medium</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        241 ~ <denied_operations>
          <!-- denied even if it is explicitly
            authorized -->
            <name>fax_send</name>
          </denied_operations>
          <operation>
            <name>net_delivery</name>
            <requirement>audit</requirement>
            242 ~ <requirement>explicit_authorization
              </requirement>
            ...
          </operation>
          <operation>
            ...
          </operation>
          243 ~ <allowed_operations> <!-- allowed without
            requirements -->
            <name>fax_receive</name>
            <name>store</name>
            ...
          </allowed_operations>
        </ace>
        <ace>
          ...
        </ace>
        ...
      </acl>
    </acc_rule>
    <acc_rule>
      <doc_category>ANY</doc_category>
      <doc_security_level>high</doc_security_level>
      <acl>
        ...
      </acl>
    </acc_rule>
  </policy>

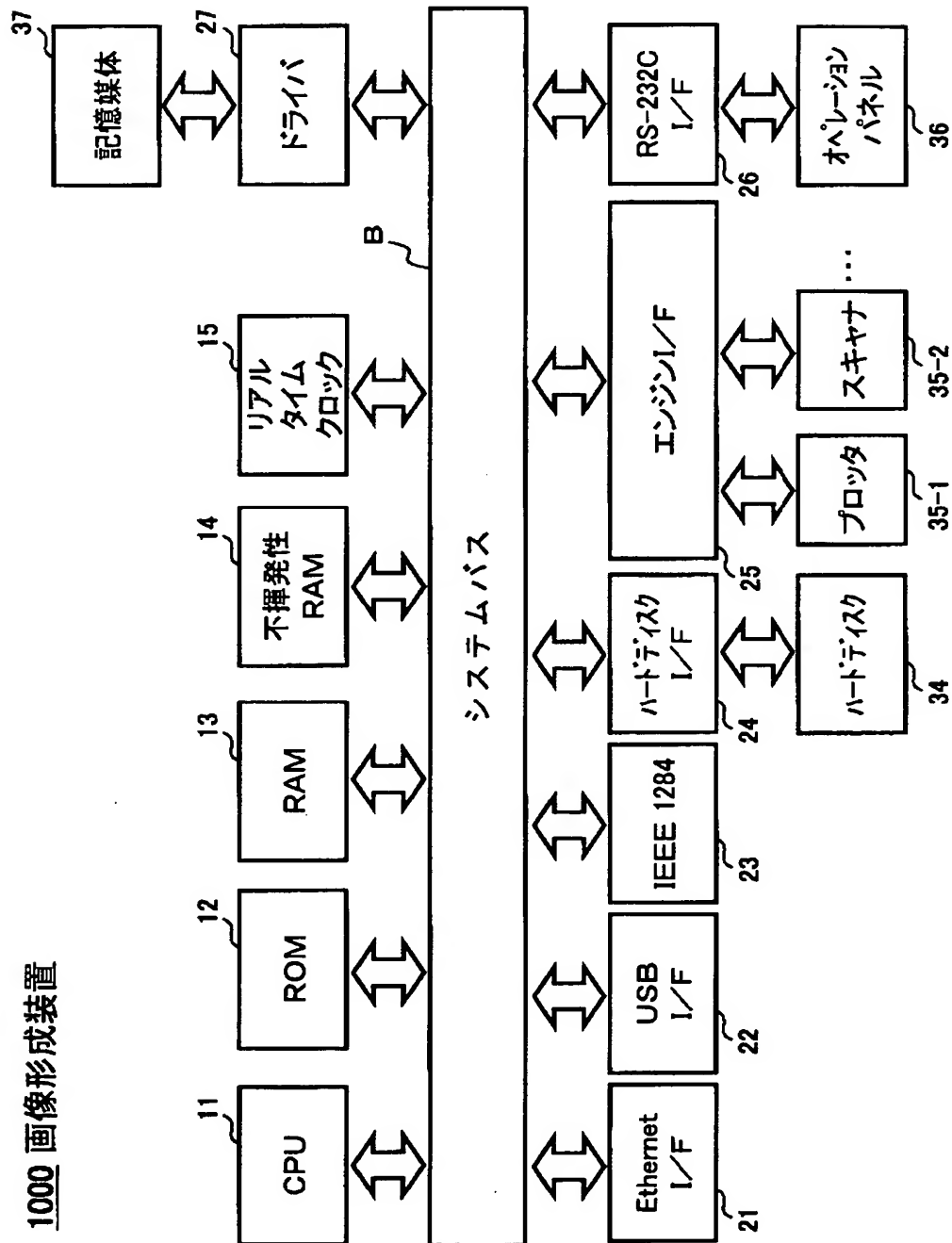
```

【図 26】

DSPを蓄積し且つ配布する種々の媒体を示す図

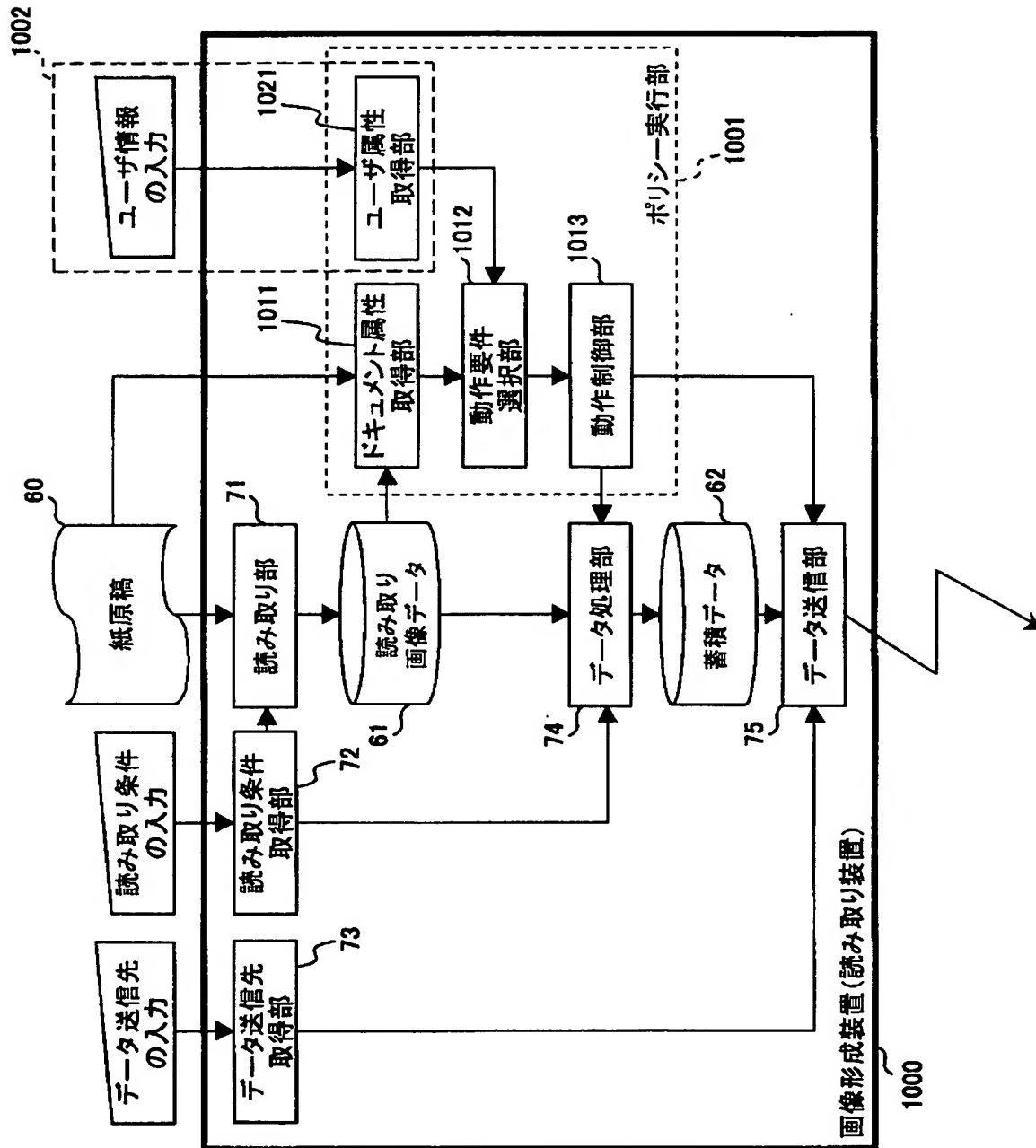


【図 27】

本発明の一実施例に係る画像形成装置の
ハードウェア構成を示すブロック図

【図 28】

セキュリティポリシーに従って動作する読み取り装置としての
画像形成装置の機能構成を示す図



【図 29】

簡略化したDSPの例を示す図

```

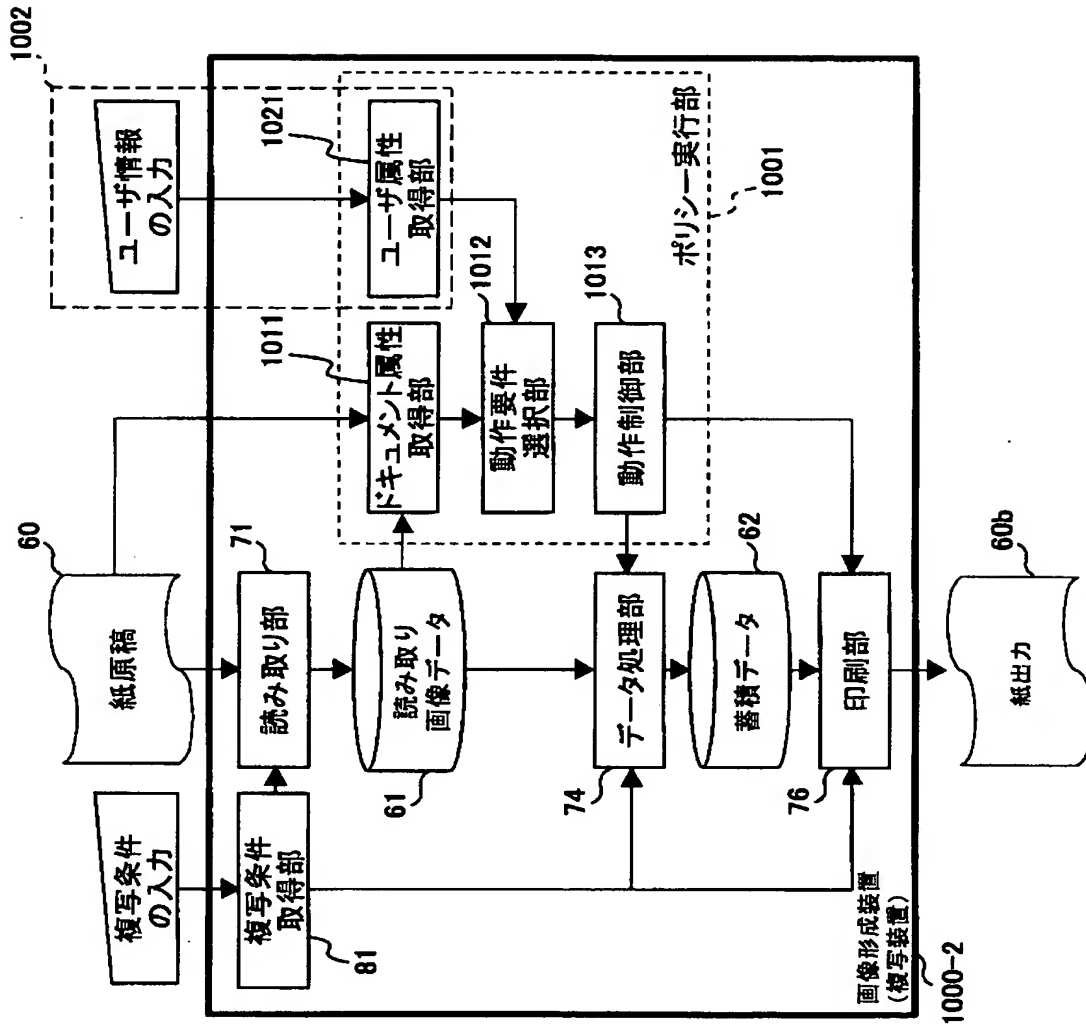
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>net_delivery</name>
          <requirement>audit</requirement>
          <requirement>print_restriction</requirement>
          <requirement>trusted_channel</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <requirement>audit</requirement>
          <requirement>embed_trace_info</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
</policy>

```

2100

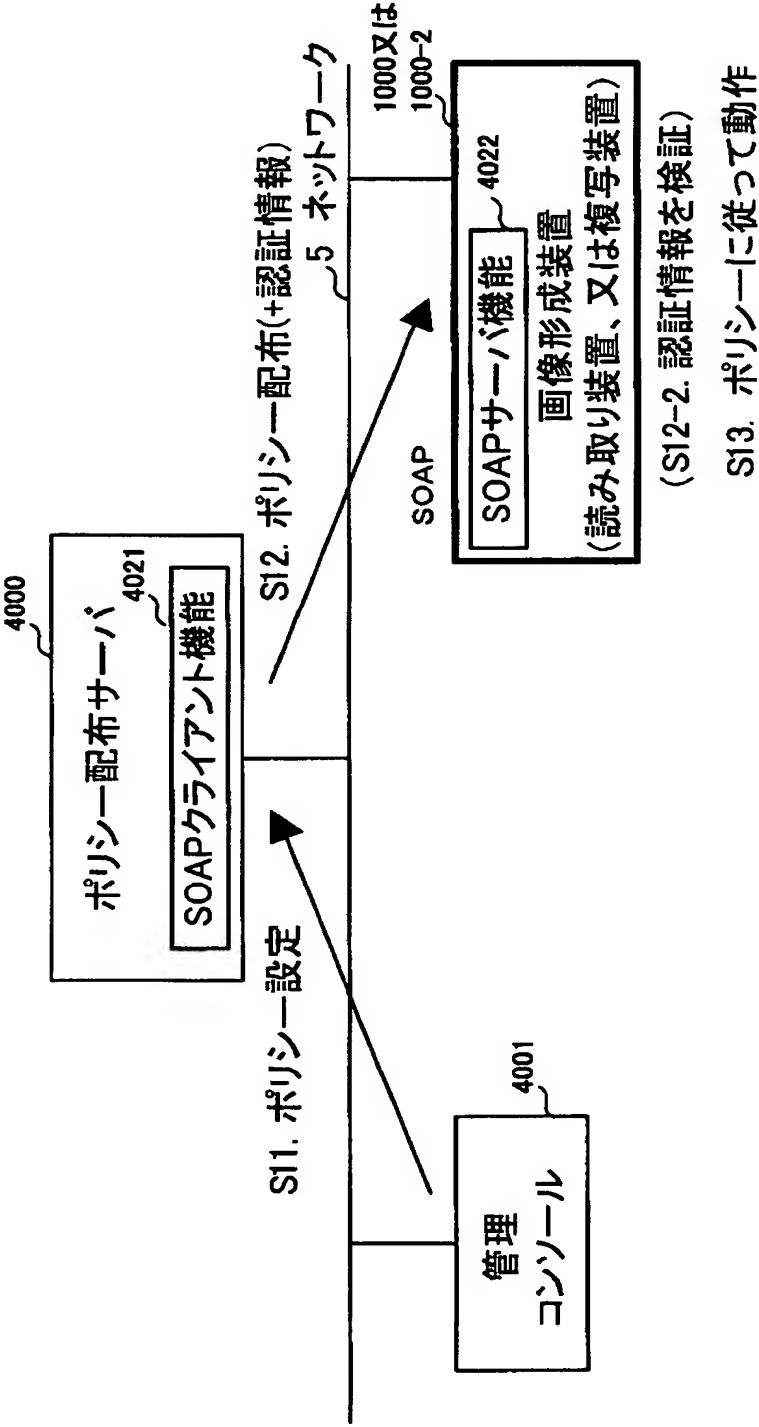
【図 30】

セキュリティポリシーに従って複写装置としての
画像形成装置の機能構成を示す図



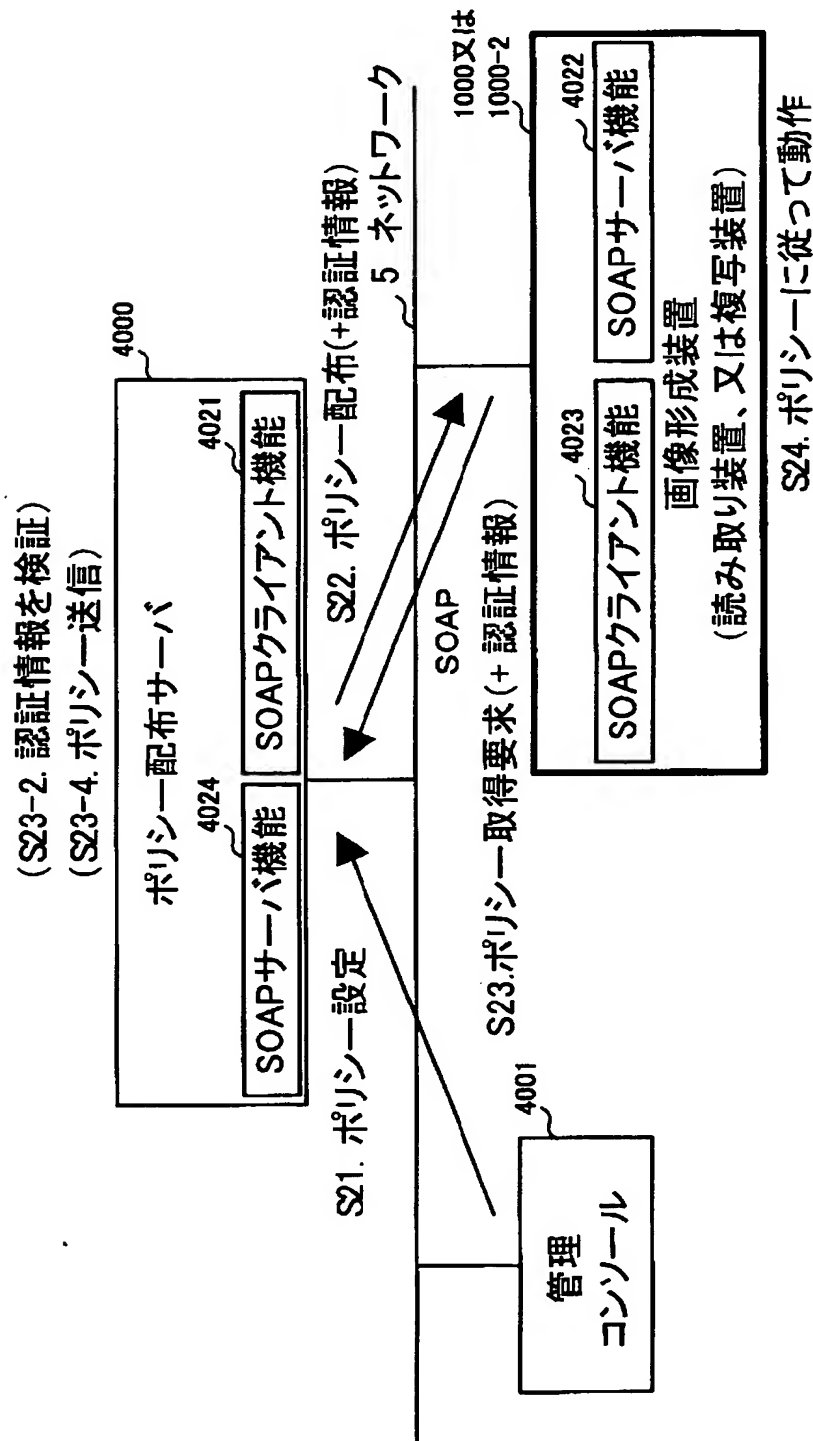
【図 3 1】

外部サーバからポリシーが配布される
第一のポリシー設定方法を示す図



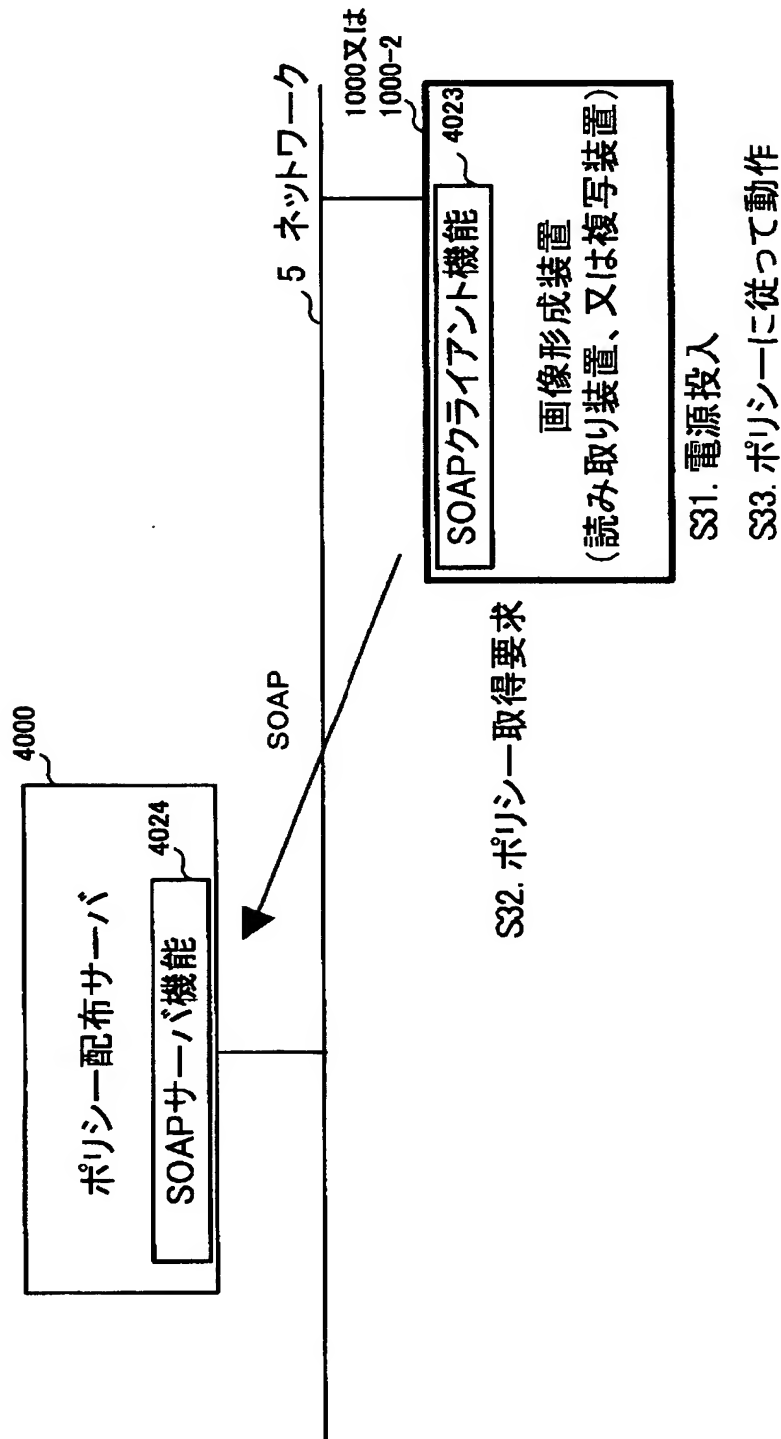
【図 3 2】

外部サーバからポリシーを取得する
第二のポリシー設定方法を示す図



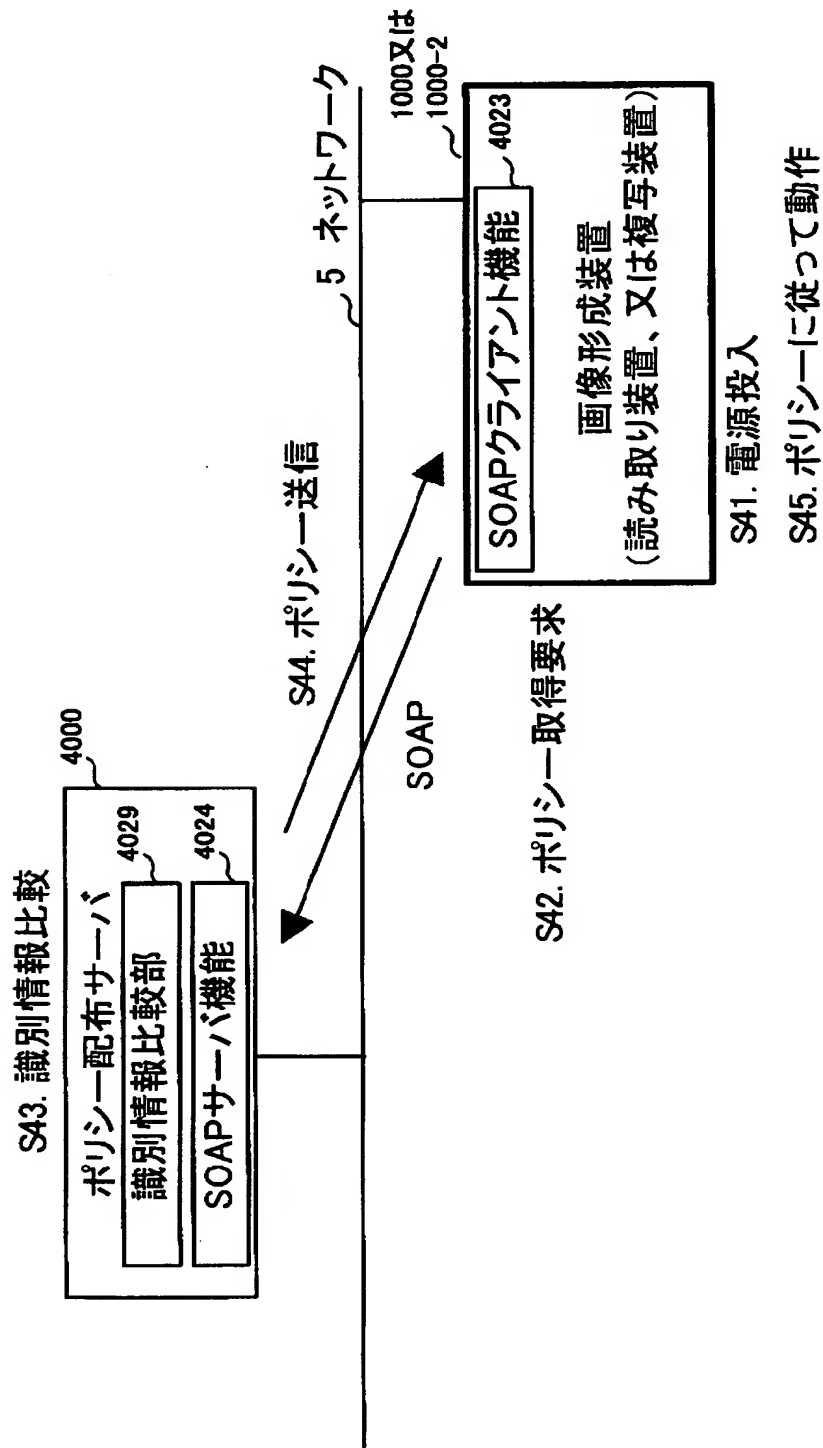
【図 33】

電源投入時にポリシーを取得する
第三のポリシー設定方法を示す



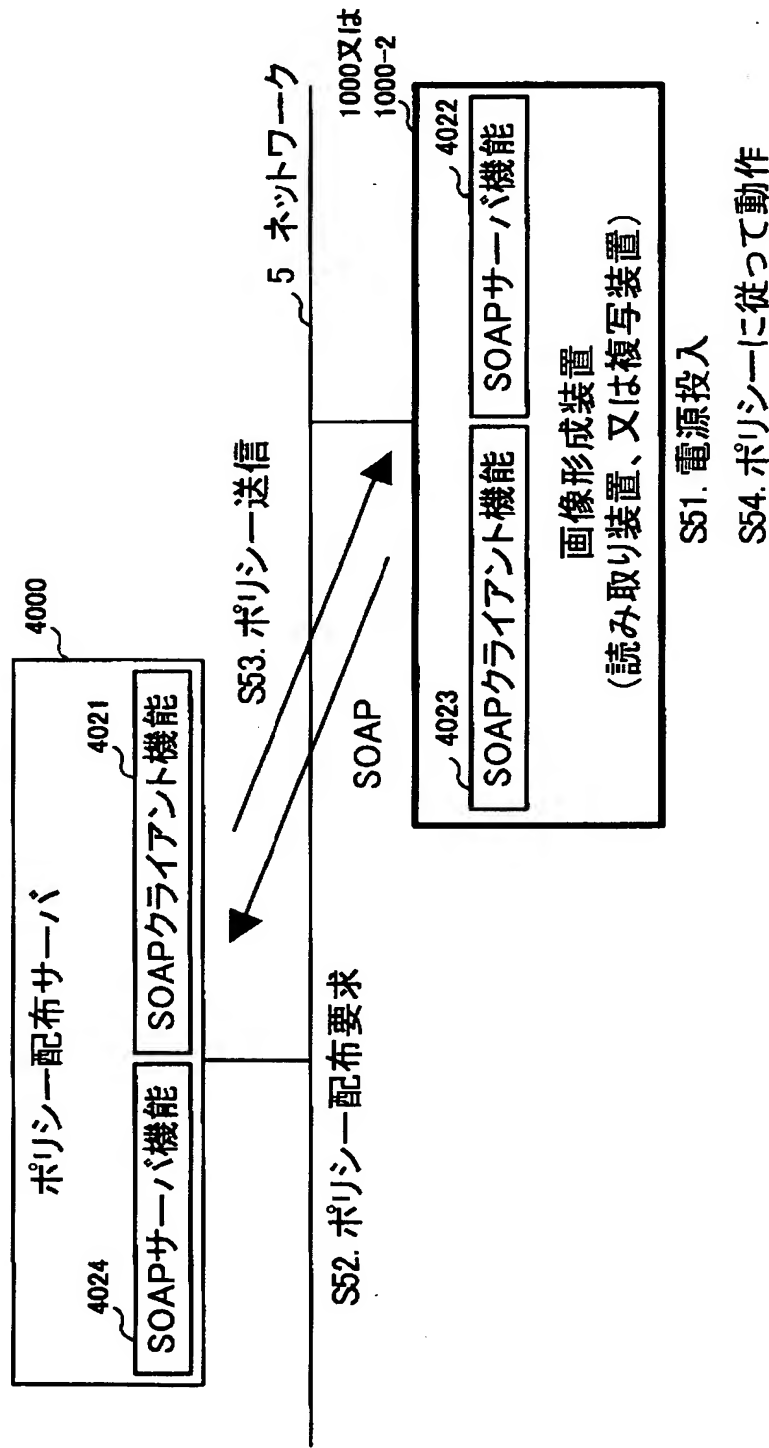
【図 3 4】

電源投入時にポリシー配布要求を行う
第四のポリシー設定方法を示す図



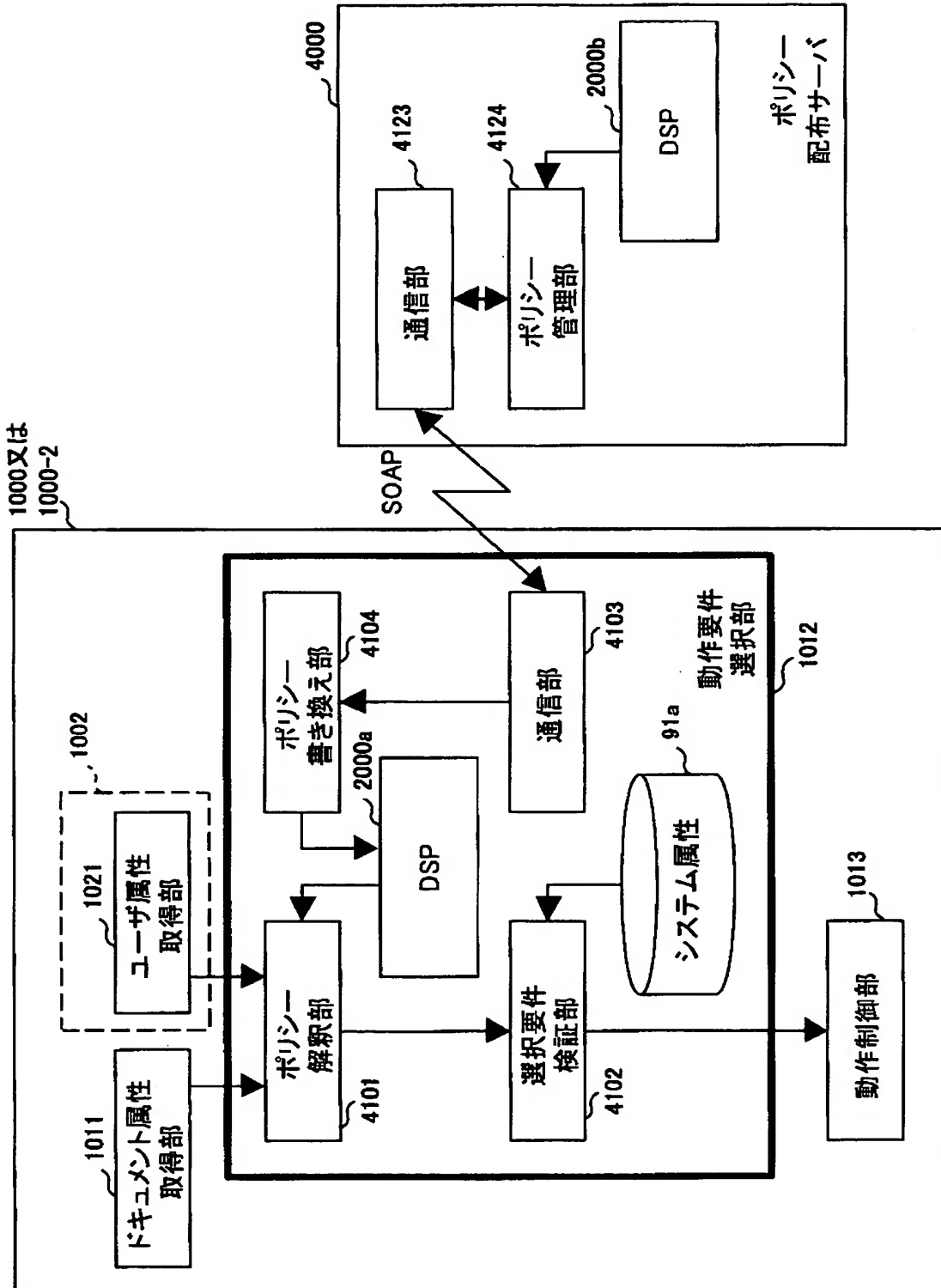
【図 35】

電源投入時にポリシー配布要求を行う
第五のポリシー設定方法を示す図



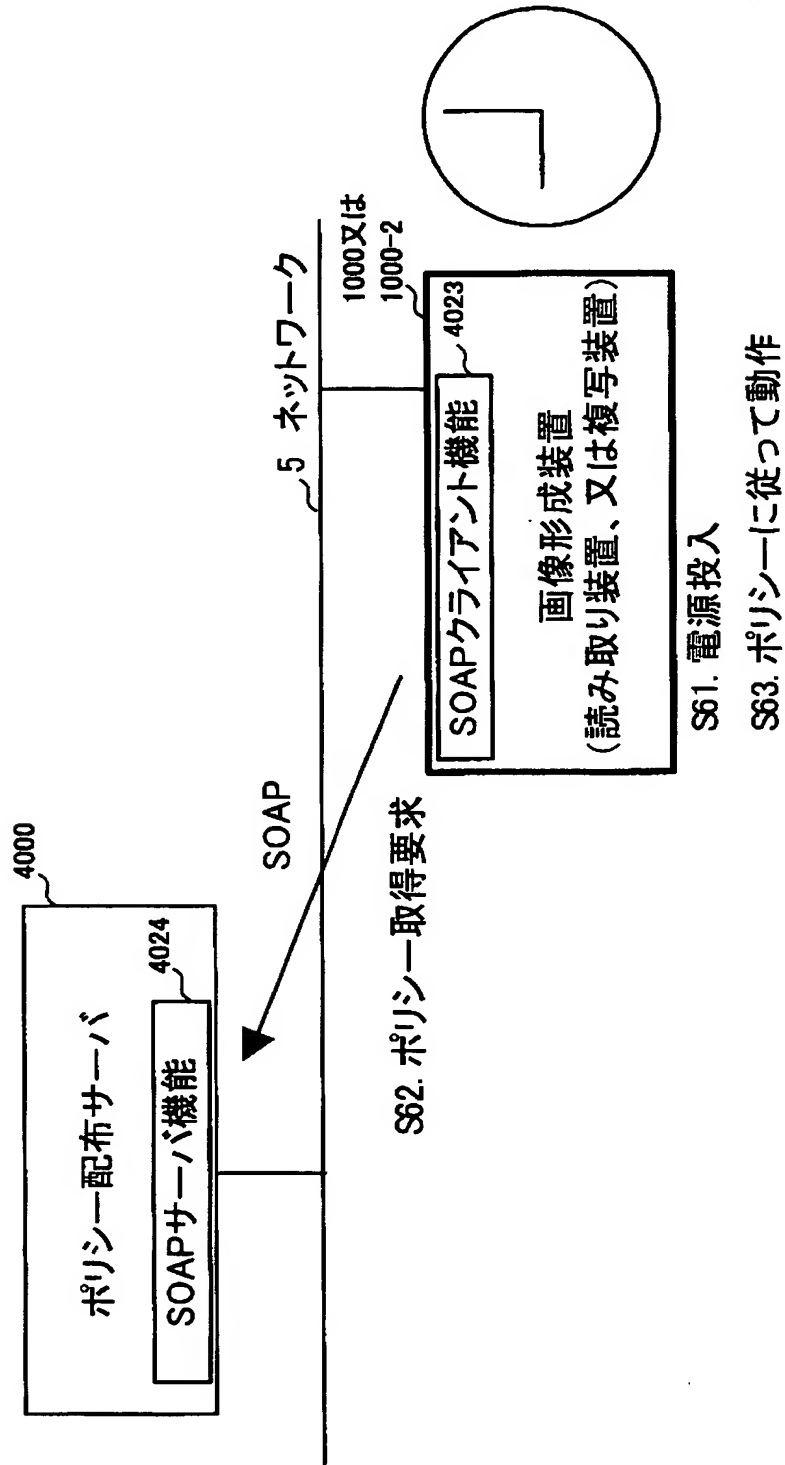
【図 36】

第一から第五のポリシー設定方法を実現するための
機能構成の例を示す図



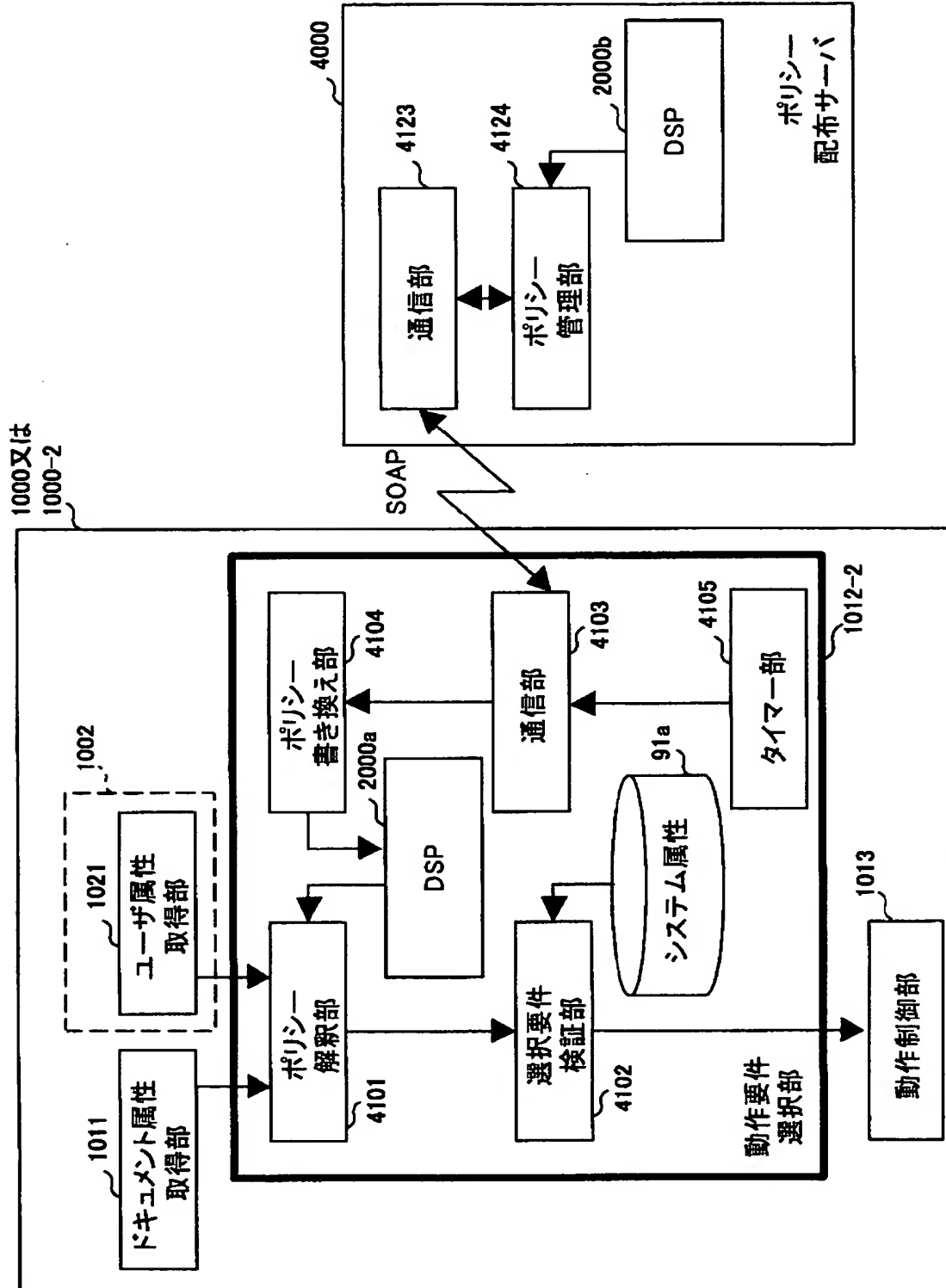
【図 37】

タイマーによってポリシーを取得する
第六のポリシー設定方法を示す図



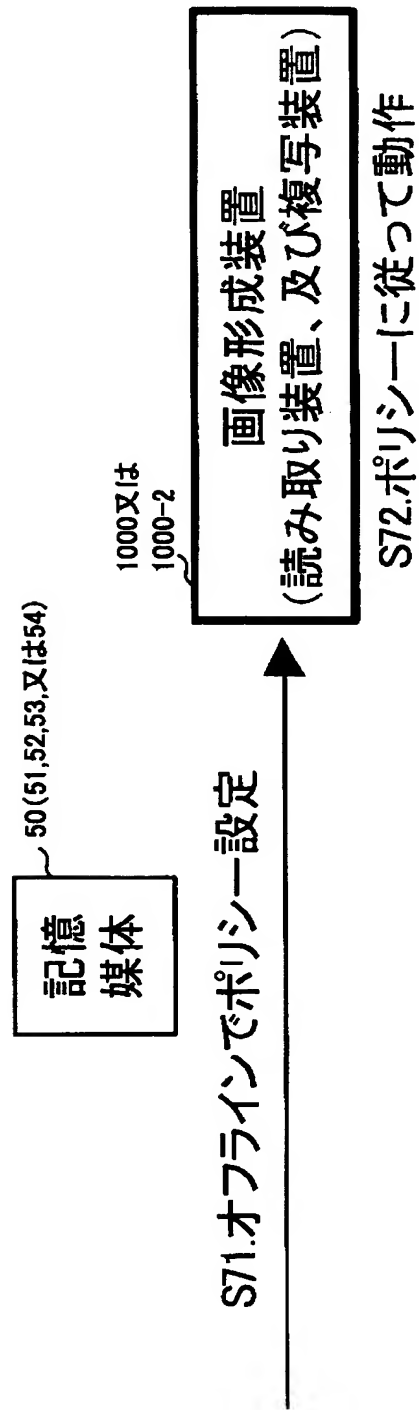
【図 38】

第六のポリシー設定方法を実現するための
機能構成の例を示す図



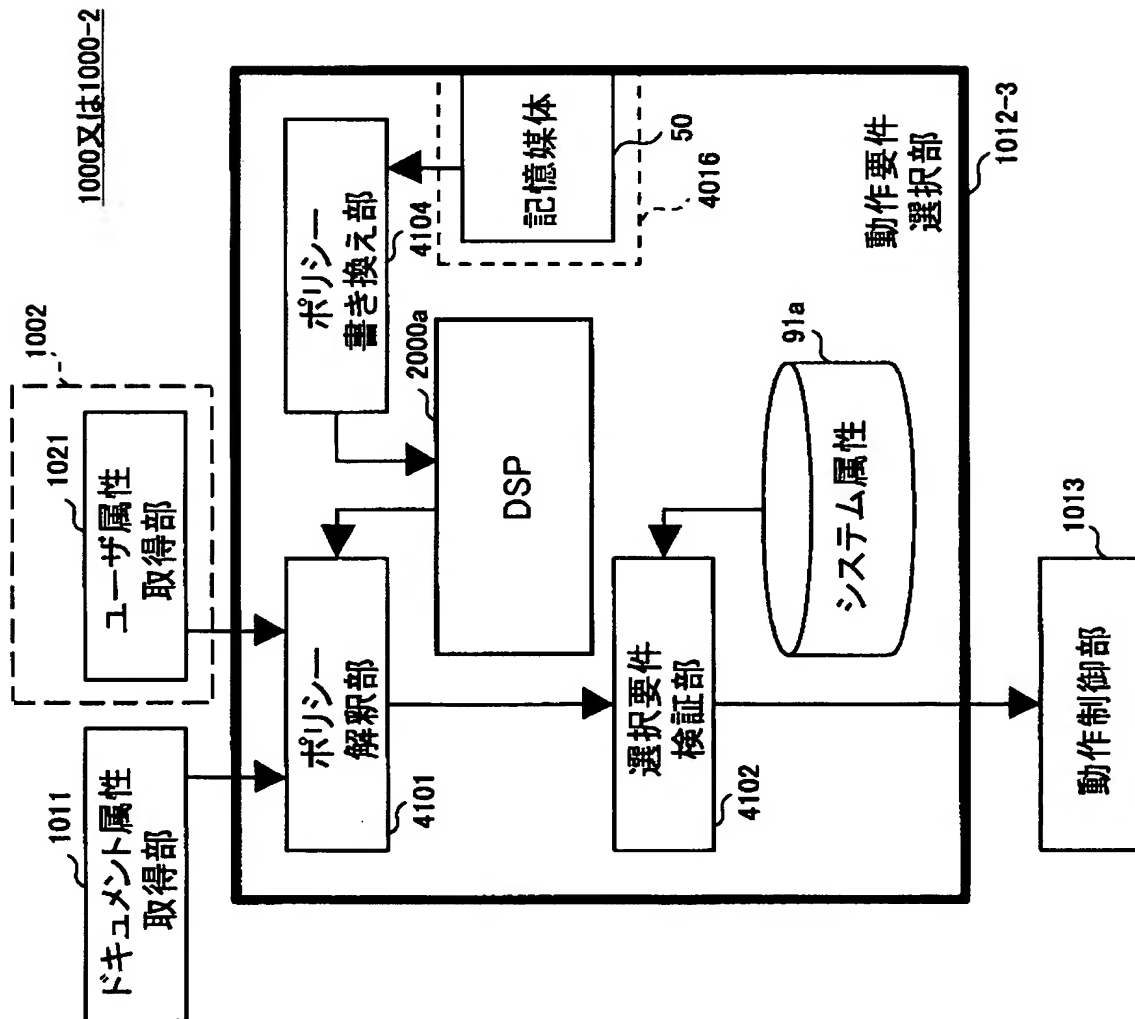
【図 39】

オフラインでポリシーを設定する
第七のポリシー設定方法を示す図



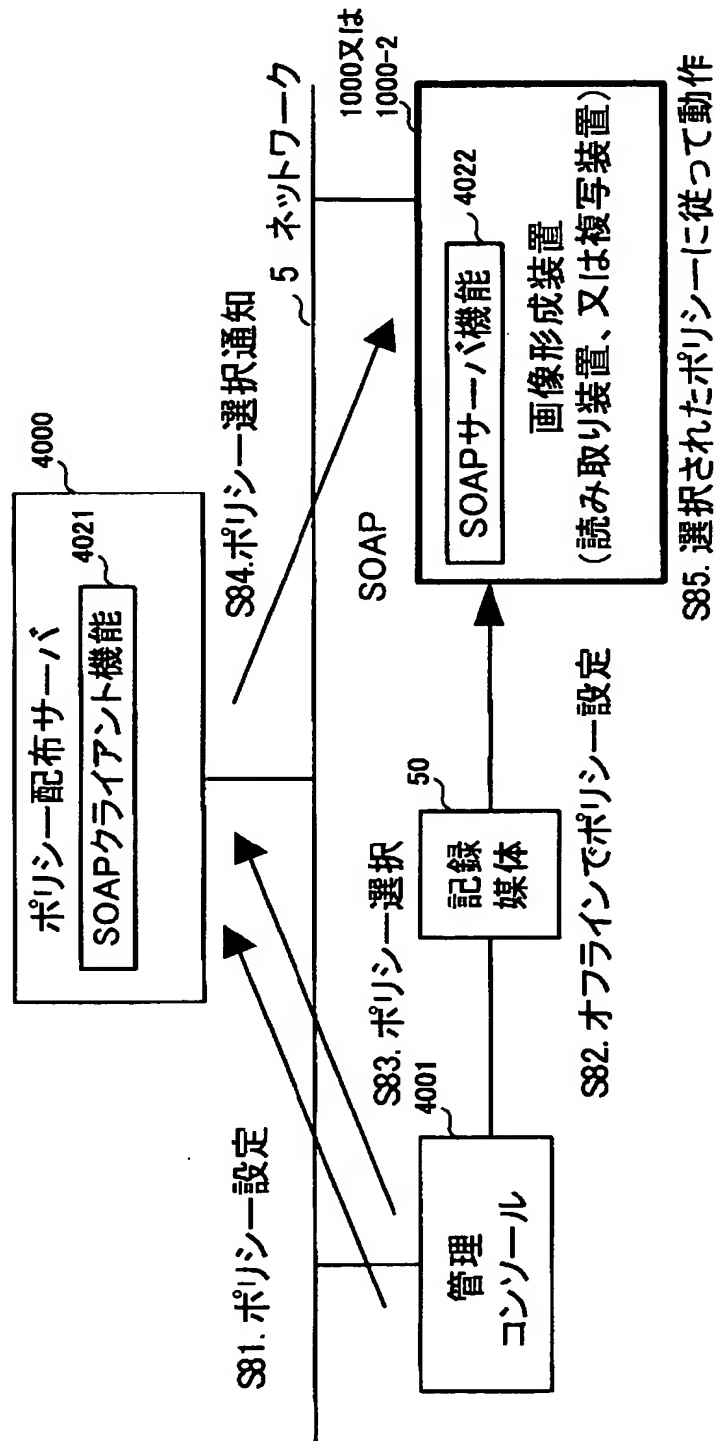
【図 40】

第六のポリシー設定方法を実現するための
機能構成の例を示す図



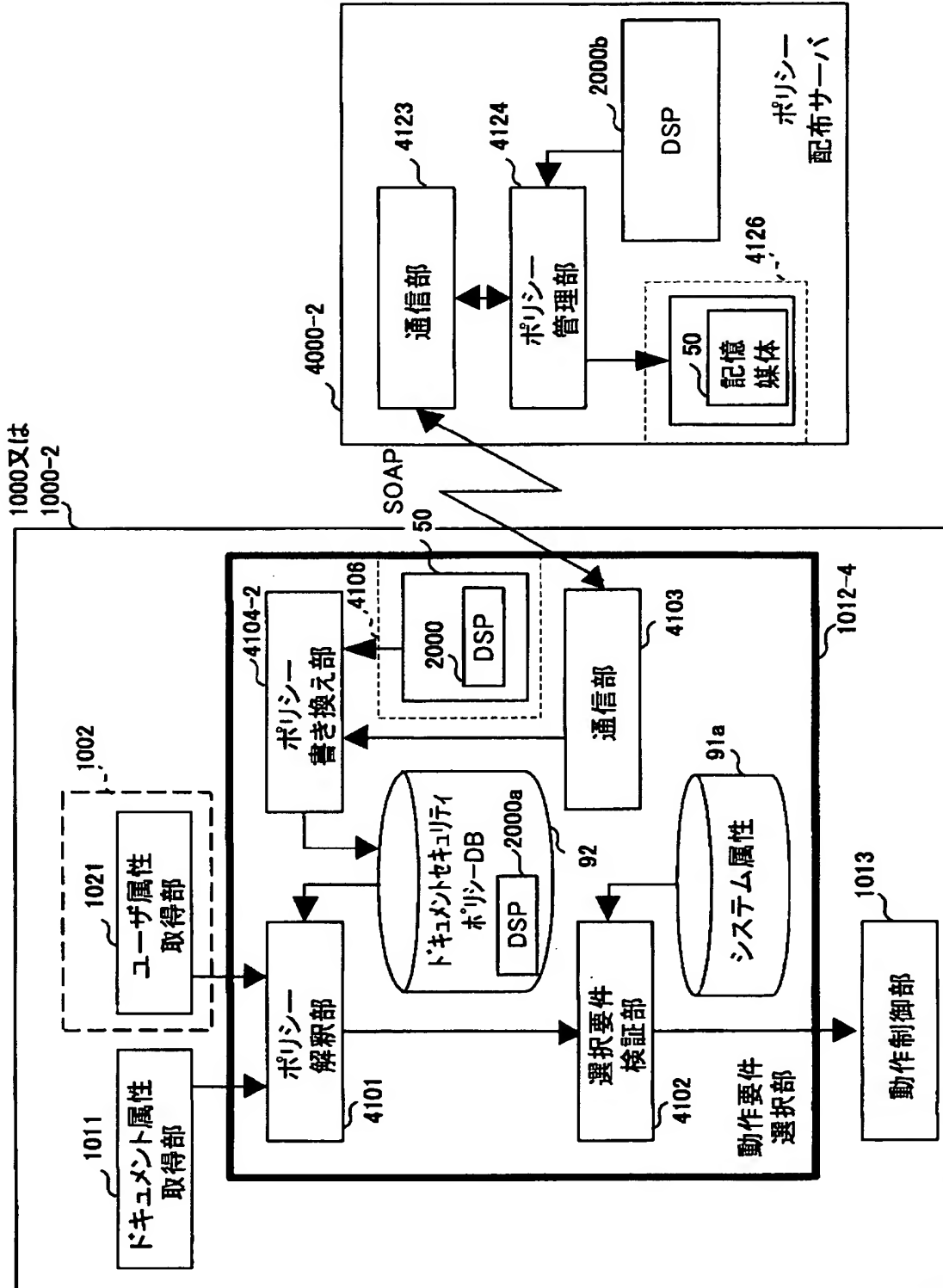
【図 41】

ポリシーをオフラインで設定し、オンラインで選択する
 第八のポリシー設定方法を示す図



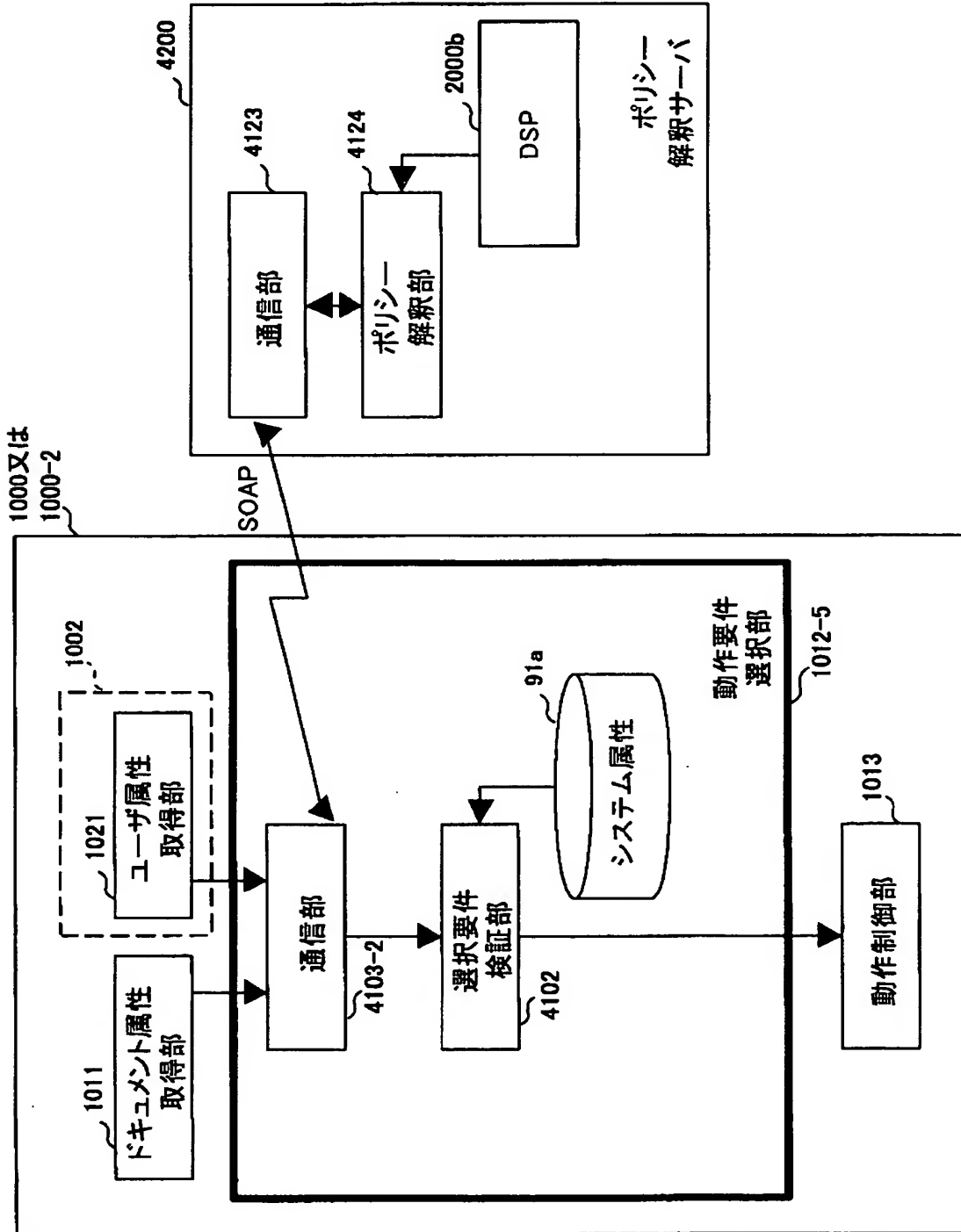
【図 42】

第八のポリシー設定方法を実現するための
機能構成の例を示す図



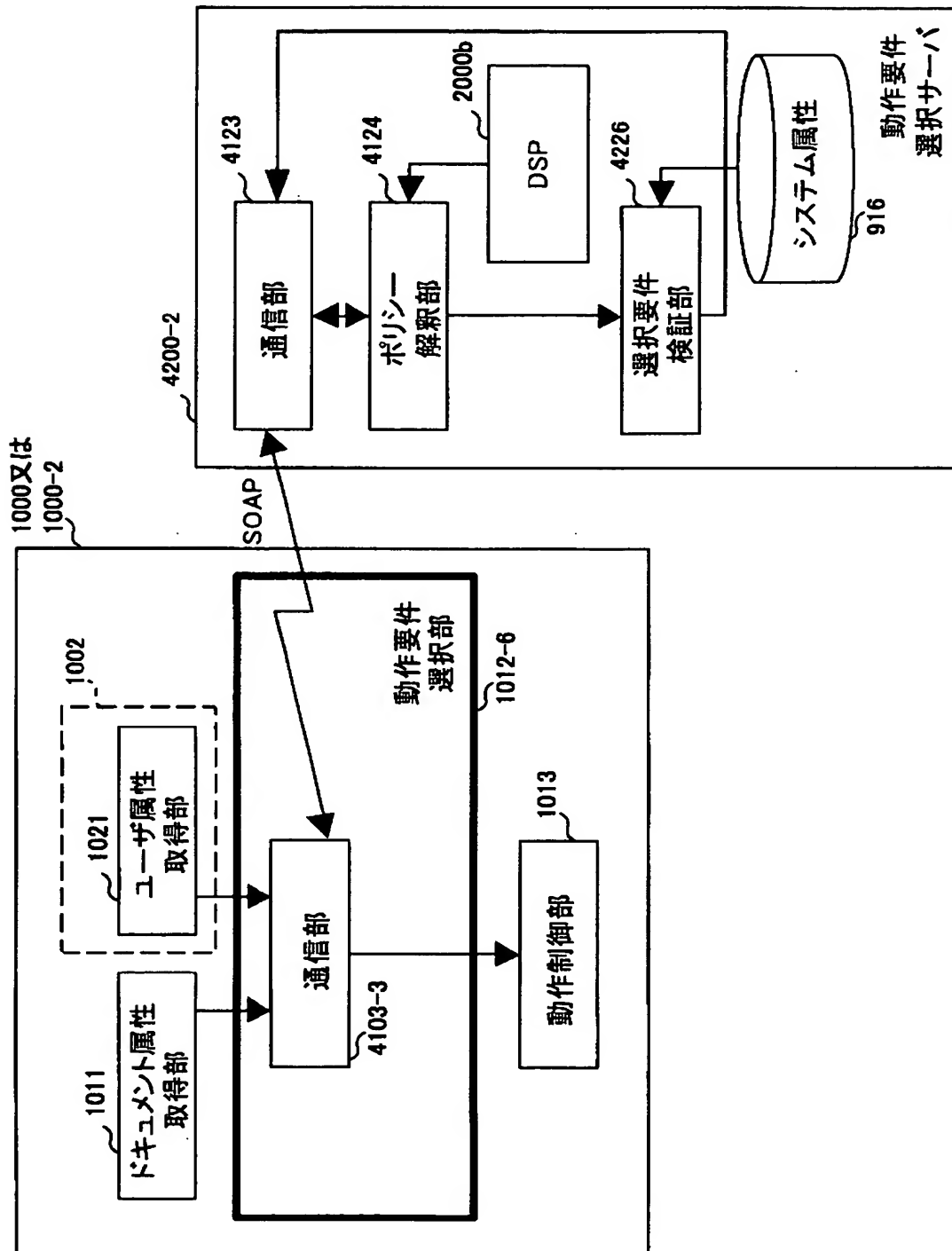
【図 43】

外部サーバがポリシーを解釈する機能構成の例を示す図



【図 4 4】

外部サーバがポリシーを解釈し、
選択要件を検証する機能構成の例を示す図



【図 4 5】

画像形成装置内に備えられたシステム属性の例を示す図

91a

動作条件	サポート
ログの記録	○
イメージログの記録	×
機密ラベルの印字	○
操作者ラベルの印字	○
識別バーコードの印字	×
識別パターンの印字	○
...	...

【図 46】

外部サーバに備えられたシステム属性の例を示す図

91b

動作条件	装置01	装置02	装置03	装置04	...
ログの記録	○	○	○	○	
イメージログの記録	×	×	○	○	
機密ラベルの印字	○	○	○	○	
操作者ラベルの印字	○	×	○	×	
識別バーコードの印字	×	×	○	×	
識別パターン印字	○	×	○	×	
...

【図 47】

SOAPに従って送信されるポリシー配布を示す
XMLデータの例を示す図

800

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistribution 801
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
      <ticket
        xsi:type="soapenc:base64"
        xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
        ANnQexdYxm/Fy7T1xwB83qXEBUicwgeVhCYu/kdcIoTcBtavhkyJtps=
      </ticket>
      <policyId xsi:type="xsd:string">RDSP2023</policyId> 803
      <policy xsi:type="xsd:string">
        ...ポリシー... 804
      </policy>
      </ns1:policyDistribution> 802
    </soapenv:Body>
  </soapenv:Envelope>

```

【図 48】

SOAPに従って送信されるポリシー配布に対する受信結果を示す
XMLデータの例を示す図

810

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistributionResponse 811
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
      <result xsi:type="xsd:boolean">true</result> 813
    </ns1:policyDistributionResponse> 812
  </soapenv:Body>
</soapenv:Envelope>
```

【図 49】

SOAPに従って送信されるポリシー配布通知を示す
XMLデータの例を示す図

820

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistributionReport ~821
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
        <ticket
          xsi:type="soapenc:base64"
          xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
          ANnQexdYxm/Fy7T1xwB83qXEBUicwgeVhCYu/kdclOTcBtavhkyJtps=
        </ticket>
        <policyId xsi:type="xsd:string">RDSP2023</policyId> ~823
      </ns1:policyDistributionReport> ~822
    </soapenv:Body>
  </soapenv:Envelope>

```

【図 50】

SOAPに従って送信されるポリシー取得要求を示す
XMLデータの例を示す図

830

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyRequest 831
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
        <ticket
          xsi:type="soapenc:base64"
          xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
          ANnQexdYxm/shuqjIKsy73kahqw520iUsJqlhHKJ/kdcIoTcBtavhkyJtps=
        </ticket>
        <policyId xsi:type="xsd:string">RDSP2023</policyId> 833
      </ns1:policyRequest> 832
    </soapenv:Body>
  </soapenv:Envelope>

```

【図 51】

SOAPに従って送信されるポリシー取得要求に対する
受信結果を示すXMLデータの例を示す図

840

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistribution 841
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
        <ticket
          xsi:type="soapenc:base64"
          xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
          </ticket>
          <policyId xsi:type="xsd:string">RDSP2023</policyId> 843
          <policy xsi:type="xsd:string">
            ...ポリシー... 844
          </policy>
        </ns1:policyDistribution> 842
      </soapenv:Body>
    </soapenv:Envelope>
  
```

【図 5 2】

SOAPに従って送信されるポリシー配布要求を示すXMLデータの例を示す図

850

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistributionRequest 851
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
      <policyId xsi:type="xsd:string">RDSP2023</policyId> 853
    </ns1:policyDistributionRequest> 852
  </soapenv:Body>
</soapenv:Envelope>
```


【図 53】

SOAPに従って送信されるポリシー選択通知を示す
XMLデータの例を示す図

```

860
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyChangeRequest ~ 861
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
        <ticket
          xsi:type="soapenc:base64"
          xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
            ANnQexdYxm/Fy7T1xwB83qXEBUicwgeVhCYu/kdcLOTcBtavhkyJtps=
          </ticket>
          <policyId xsi:type="xsd:string">RDSP2023</policyId> ~ 863
        </ns1:policyChangeRequest> ~ 862
      </soapenv:Body>
    </soapenv:Envelope>
  
```

【図 54】

SOAPに従って送信される動作要件取得要求を示す
XMLデータの例を示す図

```

870
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:isAllowed
      871
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/security/sectk">
        <userTicketInfo
          873
          xsi:type="ns2:authTicketInfo"
          xmlns:ns2="http://www.ricoh.co.jp/xmlns/schema/uauthentication"
          </targets>
          <expireDate xsi:type="xsd:dateTime">
            2003-04-02T11:29:48.796Z
          </expireDate>
          <userInfo xsi:type="ns2:principal">
            <id xsi:type="xsd:string">U:Notes:CN=Atsuhisa Saitoh,OU=R,O=RRR/id>
            <principalType xsi:type="xsd:string">user</principalType>
            <userSpace xsi:type="xsd:string">Notes</userSpace>
            <domainName xsi:type="xsd:string">RGroup</domainName>
            <name xsi:type="xsd:string">Atsuhisa Saitoh/R/RRR/name>
          </userInfo>

```

【図 55】

SOAPに従って送信される動作要件取得要求を示す
XMLデータの例を示す図

```

<groupInfo
  xsi:type="soapenc:Array"
  soapenc:arrayType="ns2:principal[1]"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
  <item>
    <id xsi:type="xsd:string">G:Notes:CN=PBDSS_USERS</id>
    <principalType xsi:type="xsd:string">group</principalType>
    <userSpace xsi:type="xsd:string">Notes</userSpace>
    <domainName xsi:type="xsd:string">RGroup</domainName>
    <name xsi:type="xsd:string">PBDSS_USERS</name>
  </item>
</groupInfo>
</userTicketInfo>
  <docInfo xsi:type="ns1:DocInfo"
    <category xsi:type="xsd:string">Technical_doc/category>
    <level xsi:type="xsd:string">High</level>
    <zone xsi:type="xsd:string">99.99.99.99</zone>
  </docInfo>
  <accessInfo
    xsi:type="ns3:AccessInfo"
    xmlns:ns3="http://www.rrr.co.jp/xmlns/schema/security/policy"
    <operation xsi:type="xsd:string">COPY</operation>
  </accessInfo>
</ns1:isAllowed>
</soapenv:Body>
</soapenv:Envelope>

```

【図 56】

SOAPに従って送信されるポリシー解釈結果を示す
XMLデータの例を示す図

890

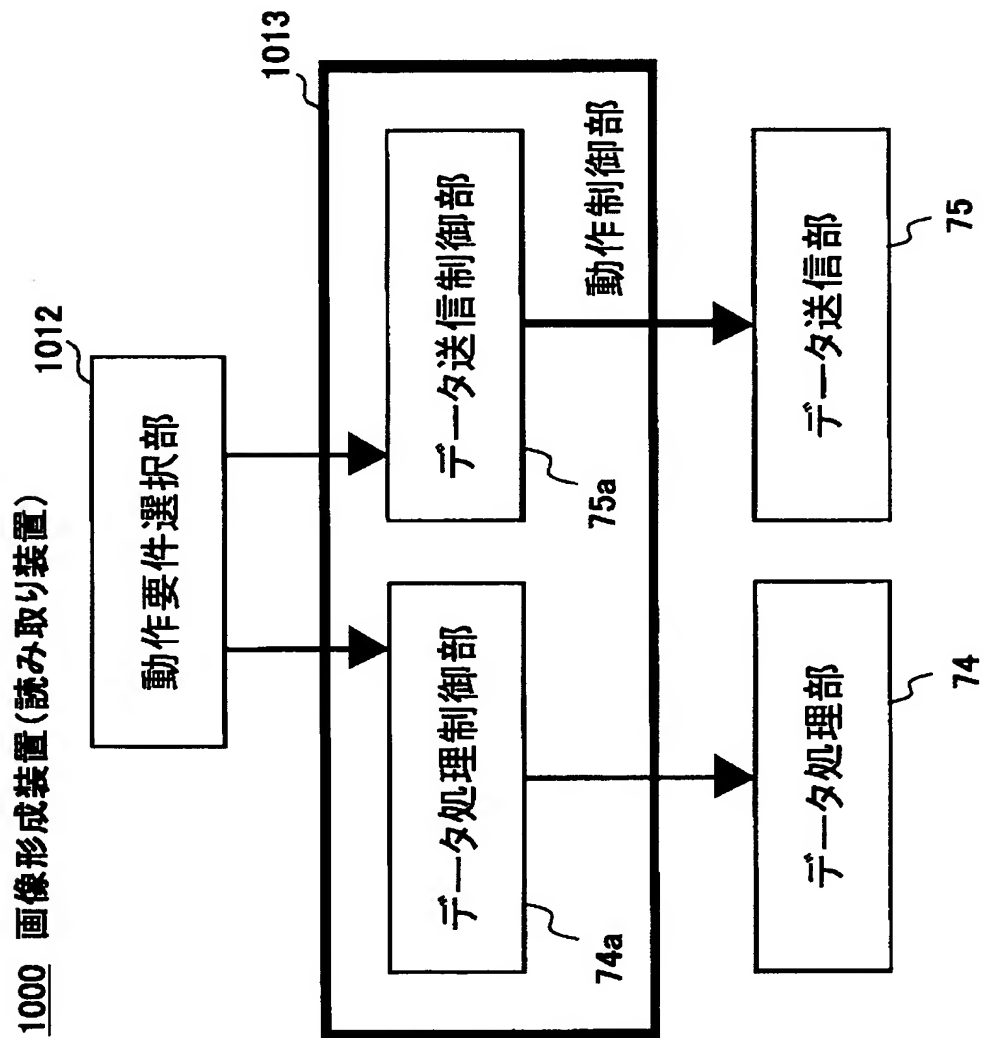
```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:isAllowedResponse 891
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/sectk">
        <isAllowedReturn
          xsi:type="ns2:DecisionInfoEx"
          xmlns:ns2="http://www.ricoh.co.jp/xmlns/schema/rdh/security/sectk">
            <allowed xsi:type="xsd:boolean">true</allowed> 895
            <requirements
              xsi:type="soapenc:Array"
              soapenc:arrayType="ns3:Requirement[1]"
              xmlns:ns3="http://www.ricoh.co.jp/xmlns/schema/rdh/security/policy"
              xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
              <item>
                <requirement xsi:type="xsd:string">audit</requirement> 897
              </item>
            </requirements>
          </isAllowedReturn> 892
        </ns1:isAllowedResponse>
      </soapenv:Body>
    </soapenv:Envelope>
  
```

896

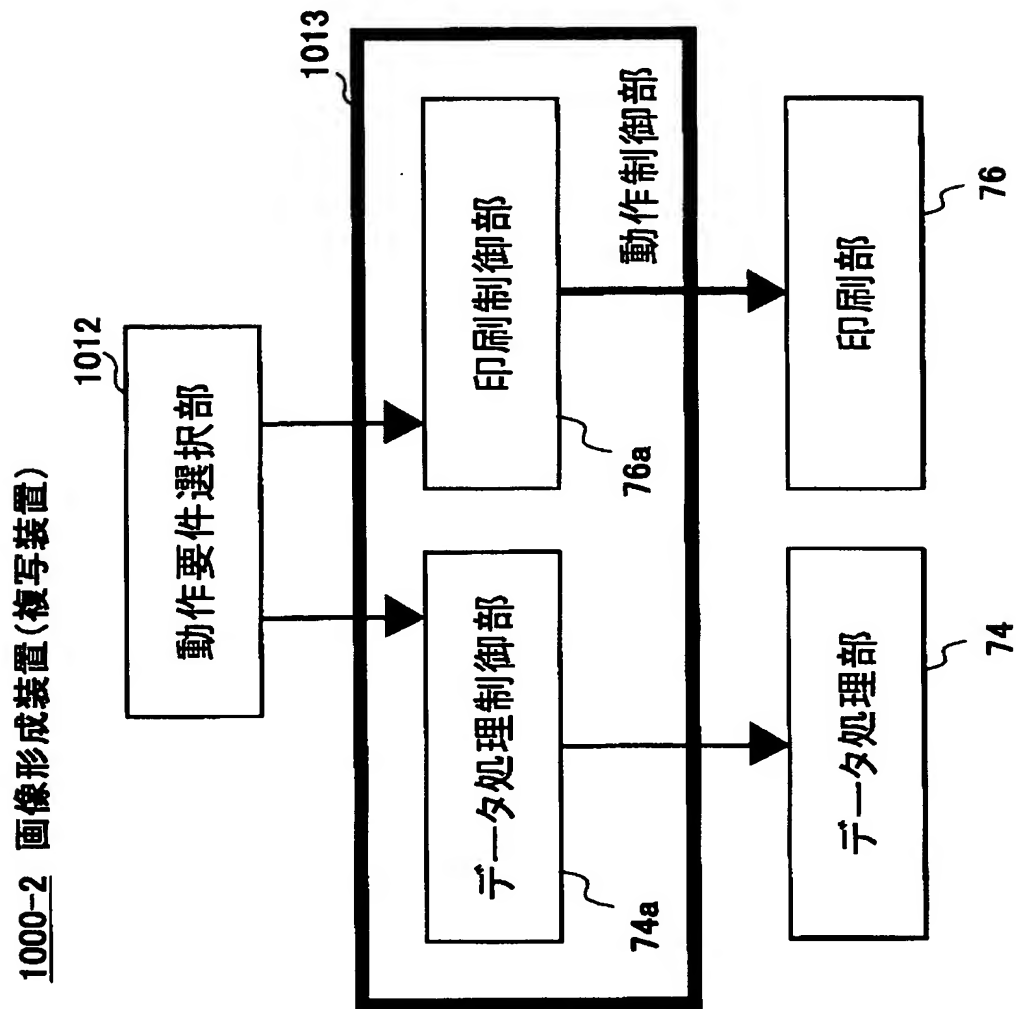
【図 57】

読み取り装置としての画像形成装置における
動作制御部の機能構成の例を示す図



【図 58】

複写装置としての画像形成装置における
動作制御部の機能構成の例を示す図



【書類名】 要約書**【要約】**

【課題】 本発明の課題は、情報システムのセキュリティを確保するシステムに関し、特に、ドキュメントのドキュメント属性を取得することによって、セキュリティポリシーに基づいた処理制御を行う画像形成装置を提供することを目的とする。

【解決手段】 本発明の課題は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手段と、外部からのセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手段と、上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有する画像形成装置によって達成される。

【選択図】 図 3 6

特願 2 0 0 3 - 3 1 4 4 6 5

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー